Journal of Algebra 473 (2017) 607–626

Contents lists available at ScienceDirect

Journal of Algebra

www.elsevier.com/locate/jalgebra

Code loops in dimension at most 8 ☆

E.A. O'Brien [a], Petr Vojtěchovský [b,*]

[a] *Department of Mathematics, University of Auckland, Private Bag 92019, Auckland, New Zealand*
[b] *Department of Mathematics, University of Denver, 2280 S Vine St, Denver, CO 80112, USA*

ARTICLE INFO

Article history:
Received 27 June 2016
Available online 24 November 2016
Communicated by William M. Kantor

MSC:
primary 20N05
secondary 15A69, 20B25, 20B40

Keywords:
Code loop
Doubly even code
Trilinear alternating form
Moufang loop
General linear group
Sporadic group
The Monster group

ABSTRACT

Code loops are certain Moufang 2-loops constructed from doubly even binary codes that play an important role in the construction of local subgroups of sporadic groups. More precisely, code loops are central extensions of the group of order 2 by an elementary abelian 2-group V in the variety of loops such that their squaring map, commutator map and associator map are related by combinatorial polarization and the associator map is a trilinear alternating form.

Using existing classifications of trilinear alternating forms over the field of 2 elements, we enumerate code loops of dimension $d = \dim(V) \leq 8$ (equivalently, of order $2^{d+1} \leq 512$) up to isomorphism. There are 767 code loops of order 128, and 80826 of order 256, and 937791557 of order 512.

☆ O'Brien was supported by the Marsden Fund of New Zealand via grant UOA 1323. Vojtěchovský was supported by Simons Foundation Collaboration Grant 210176 and 2016 PROF Grant of the University of Denver.

* Corresponding author.
E-mail addresses: e.obrien@auckland.ac.nz (E.A. O'Brien), petr@math.du.edu (P. Vojtěchovský).

http://dx.doi.org/10.1016/j.jalgebra.2016.11.006
0021-8693/

1. Introduction

Code loops are certain Moufang 2-loops constructed from doubly even binary codes that play an important role in the construction of local subgroups of sporadic groups [1,9,19].

We enumerate the code loops of order 128, 256 and 512 up to isomorphism, so extending the work of Nagy and Vojtěchovský [26]. The results are summarized in Tables 1 and 2. The code loops can be constructed explicitly; those of orders dividing 256 will be available in a future release of the LOOPS package [27] for GAP [13].

The theoretical results required for the classification of code loops were described briefly in [26], in the context of a larger project of enumerating all Moufang loops of order 64. Since our work suggests that it will be difficult to extend the classification of code loops beyond order 512 (see Remark 4.1), we carefully record the theory here.

In Section 2 we recall the necessary background material on Moufang loops, code loops, symplectic 2-loops, trilinear alternating forms, combinatorial polarization and small Frattini Moufang loops. In particular, we recall that code loops, symplectic Moufang 2-loops and small Frattini Moufang 2-loops are the same objects. The group $GL(V)$ acts naturally on the set F^V of maps $V \to F$ by

$$f \mapsto f^S, \quad f^S(u) = f(uS^{-1}).$$

We show that two code loops, realized as central extensions of the two-element field $F = \mathbb{F}_2$ by a vector space V over F, are isomorphic if and only if their squaring maps $x \mapsto x^2$ (which can be realized as maps $V \to F$) lie in the same orbit of this action.

For $f \in F^V$ with $f(0) = 0$, the mth derived form f_m of f is the symmetric map $V^m \to F$ defined by

$$f_m(v_1, \dots, v_m) = \sum_{\emptyset \neq I \subseteq \{1,\dots,m\}} (-1)^{m-|I|} f(\sum_{i \in I} v_i). \tag{1.1}$$

If $P : V \to F$ is the squaring map of a code loop Q, then $P_2 = C : V^2 \to F$ is the commutator map of Q, $P_3 = A : V^3 \to F$ is the associator map of Q, and $P_4 = 0$. Let

$$F_4^V = \{f \in F^V \mid f(0) = 0,\ f_4 = 0\},$$

so that F_4^V consists of maps $f : V \to F$ such that f_3 is a trilinear alternating form. The results of Section 2 imply that $f \in F^V$ is the squaring map of a code loop if and only if $f \in F_4^V$.

In Section 3 we therefore study the action of $GL(V)$ on F^V restricted to F_4^V, whose orbits are in one-to-one correspondence with code loops of order $n = 2^{\dim(V)+1}$ up to isomorphism. Suppose that V has ordered basis $(e_1, \dots, e_d)$. A map $f \in F_4^V$ is uniquely determined by the values

$$\omega_{i_1 \cdots i_k} = f_k(e_{i_1}, \dots, e_{i_k}) \in F, \tag{1.2}$$