J Algebr Comb (2010) 31: 585–611
DOI 10.1007/s10801-009-0203-2

Code loops in both parities

Aleš Drápal · Petr Vojtěchovský

Received: 7 April 2009 / Accepted: 1 September 2009 / Published online: 24 September 2009

Abstract We present equivalent definitions of code loops in any characteristic $p \neq 0$. The most natural definition is via combinatorial polarization, but we also show how to realize code loops by linear codes and as a class of symplectic conjugacy closed loops. For p odd, it is possible to define code loops via characteristic trilinear forms. Related concepts are discussed.

Keywords Code loop · Even code loop · Odd code loop · Symplectic loop · Small Frattini loop · Moufang loop · Conjugacy closed loop · Combinatorial polarization · Symmetric associator · Characteristic form · Doubly even code · Self-orthogonal code · Kronecker product

1 Introduction

The largest sporadic group, the *Monster*, was discovered by Griess in [14], [15], and its simplest known construction is due to Conway [5]. One of the crucial steps in Conway's construction is a transition from the extended binary Golay code $\mathcal{G}$ to a certain loop $\mathcal{P}$, called the *Parker loop*, consisting of signed elements of $\mathcal{G}$. The additions in $\mathcal{P}$ and $\mathcal{G}$ are the same, except that the sign arithmetic in $\mathcal{P}$ is governed by

A. Drápal supported by Grant Agency of the Czech Republic grant 201/09/0296. A preliminary version of this paper was written while A. Drápal was visiting University of Wisconsin-Madison as a Fulbright research scholar. P. Vojtěchovský partially supported by Eduard Čech Center grant LC505.

A. Drápal
Department of Algebra, Charles University, Sokolovská 83, 186 75 Prague, Czech Republic
e-mail: drapal@karlin.mff.cuni.cz

P. Vojtěchovský (✉)
Department of Mathematics, University of Denver, 2360 S Gaylord St, Denver, CO 80208, USA
e-mail: petr@math.du.edu

rather delicate rules based on the code structure of $\mathcal{G}$. See [5] or [6, Chapter 29] for details.

In [16], Griess showed that an analogous transition from a code to a loop can be done for any doubly even linear binary code, resulting in a class of Moufang loops, called *even code loops* here. (Griess called them *code loops*.)

Even code loops have been studied extensively, as witnessed by: characterization of even code loops by means of combinatorial polarization [1, Section 13], characterization of even code loops as Moufang loops with a unique nonidentity square [3], characterization of even code loops as small Frattini Moufang 2-loops [17], calculation of the sign within even code loops [18], [23], construction of 2-local subgroups of sporadic groups from even code loops [1, Section 14], classification of small even code loops [24].

In order to construct p-local subgroups of the Monster for $p = 3$, 5 and 7, Richardson [29] gave a definition of an *odd code loop* based on self-orthogonal codes over $\mathbb{F}_p$. He also pointed out similarities between the even and odd code loops, notably a connection to combinatorial polarization.

Motivated by Richardson's pioneering work, this paper is an attempt to arrive at the "correct" definition of code loops in any characteristic $p \neq 0$. While the definition of even code loops has been settled, we argue that Richardson's definition of odd code loops should be generalized to more closely resemble the even case.

To wit, we present three equivalent ways in which odd and even code loops can be defined: via combinatorial polarization, via linear codes, and as a class of symplectic conjugacy closed p-loops. When p is odd, another equivalent definition is via characteristic trilinear forms.

Although equivalent, the four definitions are somewhat heterogeneous and depend on concepts from several different areas, which we gather in Section 2. The definitions are then given in Section 3. The classical case of even code loops can be found in Section 4, with several novel proofs. Our goal in Section 4 is not to give the most elementary proofs, but to take advantage of well-known results in loop theory. A certain universal code construction is presented in Section 5. We use it in Section 6 to show the equivalence of definitions for odd code loops via codes and via forms, and also to compare our definition with Richardson's original definition of odd code loops. Odd code loops via forms are shown to be equivalent to odd code loops via polarization in Section 7, and via conjugacy closed loops in Section 8. We briefly discuss properties of code loops and the isomorphism problem for code loops in Section 9. Finally, Section 10 offers several insights into the four equivalent definitions, and explores related concepts.

It is our expressed hope that the algebraic foundations of code loops developed in this paper will eventually lead to a better understanding of p-locals in sporadic groups—a topic that is not pursued here.

2 Prerequisites

Throughout the paper, p is a prime, $\mathbb{F}_p$ is the p-element field, $\mathbb{Z}_p$ is the cyclic group of order p, and all algebras are finite. Unless otherwise stated, all sums are taken over *all* subscripts appearing in the summands. For instance, $\sum a_k$ is the sum over all k, and $\sum_{i<j} a_i b_j c_k$ is the sum over all i, j, k such that $i < j$, where the domains for i, j, k are understood from the context.

2.1 Loops

A *quasigroup* Q is a set with a binary operation, written as juxtaposition, such that every *left translation* $L_x : Q \to Q$, $y \mapsto xy$ and every *right translation* $R_x : Q \to Q$, $y \mapsto yx$ is a bijection of Q. A *loop* is a quasigroup Q with *neutral element*, i.e., an element $1 \in Q$ such that $1x = x1 = x$ for every $x \in Q$. Note that groups are precisely associative loops.

To save space and improve legibility, we use the *dot convention* to indicate priority of multiplication. For instance, $xy \cdot z$ stands for $(xy)z$.

Let Q be a loop. For x, $y \in Q$, let $L(x, y) = L_{yx}^{-1} L_y L_x$, $R(x, y) = R_{xy}^{-1} R_y R_x$, and $T(x) = L_x^{-1} R_x$ be the *inner mappings* of Q. A subloop H of Q is *normal* if it is invariant under all inner mappings of Q. In such a case we write $H \trianglelefteq Q$, and Q/H is the usual *factor loop* Q modulo H.

The *commutator* of x, $y \in Q$ is the unique element $[x, y] \in Q$ such that $xy = yx \cdot [x, y]$. The *associator* of $x, y, z \in Q$ is the unique element $[x, y, z] \in Q$ such that $(xy)z = x(yz) \cdot [x, y, z]$. We also introduce the *commutator mapping* $C : Q^2 \to Q$, $(x, y) \mapsto [x, y]$ and the *associator mapping* $A : Q^3 \to Q$, $(x, y, z) \mapsto [x, y, z]$. When there is a normal subloop H of Q such that $C(x, y) = C(x', y')$ and $A(x, y, z) = A(x', y', z')$ whenever $xH = x'H$, $yH = y'H$ and $zH = z'H$, we can view C and A as mappings from $(Q/H)^2$ and $(Q/H)^3$, respectively.

The *nucleus* of Q is the subloop $N(Q) = \{x \in Q;\ [x, y, z] = [y, x, z] = [y, z, x] = 1$ for every y, $z \in Q\}$. The *center* of Q is the normal subloop $Z(Q) = \{x \in N(Q);\ [x, y] = [y, x] = 1$ for every $y \in Q\}$.

A loop Q is *conjugacy closed* if $L_x^{-1} L_y L_x$ is a left translation and $R_x^{-1} R_y R_x$ is a right translation of Q for every x, $y \in Q$. A loop Q is *Moufang* if $x(y(xz)) = ((xy)x)z$ holds, and *extra* if $x(y(zx)) = ((xy)z)x$ holds in Q. A loop is *diassociative* if every two of its elements generate an associative subloop. Moufang loops are diassociative.

For a loop Q, let $Z_0(Q) = 1$, and let $Z_{i+1}(Q)$ be the unique normal subloop of Q containing $Z_i(Q)$ such that $Z_{i+1}(Q)/Z_i(Q) = Z(Q/Z_i(Q))$. Then $Z_1(Q) = Z(Q)$, $Z_i(Q) \trianglelefteq Z(Q)$ for every i, and $1 = Z_0(Q) \le Z_1(Q) \le Z_2(Q) \le \cdots$ is the *upper central series* of Q. We say that Q is (*centrally*) *nilpotent of class n* if n is the least integer such that $Z_n(Q) = Q$.

Given a normal subloop H of Q, let (H, Q) be the intersection of all normal subloops K of Q such that $HK/K \le Z(Q/K)$. Define $Q_0 = Q$, and $Q_{i+1} = (Q_i, Q)$. Then $Q_i \trianglelefteq Q$ for every i, and $Q = Q_0 \ge Q_1 \ge Q_2 \ge \cdots$ is the *lower central series* of Q. The normal subloop $Q_1 = (Q, Q)$ is also denoted by Q', and it is the least normal subloop H of Q such that Q/H is an Abelian group.

By a result of Bruck [2, Lemma VI.1.2], the upper and lower central series interact in a way familiar from group theory. That is, if $Q_{\beta+1} \subseteq Z_{\alpha+1}(Q)$ for some α and β, then also $Q_\beta \subseteq Z_{\alpha+2}(Q)$ and $Q_{\beta+2} \subseteq Z_\alpha(Q)$.

A *p-loop* is a loop of order p^a for some $a \ge 0$. For Moufang loops, this is equivalent to the condition that the order of every element is a power of p.

A bijection $f : Q \to Q$ is a *(right) pseudoautomorphism with (right) companion* $c \in Q$ if $f(xy)c = f(x) \cdot f(y)c$ holds for every $x, y \in Q$.

For an introduction to the theory of loops, see [2] and [26].

2.2 Central extensions of loops

There is no loop-theoretical analog to Schreier's results on group extensions, but central extensions of loops generalize from groups easily. For more about loop extensions, see [19], [10], [21], and [25].

Anticipating a more special situation, let F, V be loops. Then Q is an *extension of* F *by* V if $F \trianglelefteq Q$ and Q/F is isomorphic to V. The extension is *central* if $F \leq Z(Q)$.

Given an Abelian group F and a loop V, a mapping $\theta : V^2 \to F$ is a *cocycle* if $\theta(1, v) = \theta(v, 1) = 1$ for every $v \in V$. For a cocycle $\theta : V^2 \to F$, denote by V_θ the groupoid defined on $F \times V$ by

$$(a, u)(b, v) = (ab\theta(u, v), uv). \tag{2.1}$$

It is not hard to see that V_θ is a loop with neutral element $(1, 1)$ and $F \leq Z(V_\theta)$. Thus V_θ is a central extension of F by V. In fact, every central extension arises in this way, cf. [2]:

Theorem 2.1 *Let F be an Abelian group and V a loop. The following conditions are equivalent*:

(i) *Q is a central extension of F by V*,
(ii) *$Q = V_\theta$ for some cocycle $\theta : V^2 \to F$.*

We will mostly deal with extensions of the Abelian group of a field F by a vector space V over F. In such a case, we write the loop operations in F and V additively, and hence the multiplication in V_θ is given by

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

If θ is clear from the context, we denote the commutator and associator mappings in V_θ by C and A, as in Subsection 2.1. Else we use C_θ and A_θ for emphasis.

A straightforward calculation yields:

Lemma 2.2 *Let $Q = V_\theta$, where V is a vector space over F and $\theta : V^2 \to F$ is a cocycle. Then the commutator mapping C can be viewed as a mapping $V^2 \to F$ and the associator mapping A can be viewed as a mapping $V^3 \to F$, namely*

$$C(u, v) = \theta(u, v) - \theta(v, u), \tag{2.2}$$

$$A(u, v, w) = \theta(u, v) + \theta(u + v, w) - \theta(v, w) - \theta(u, v + w) \tag{2.3}$$

for every $u, v, w \in V$.

2.3 Symplectic p-loops and small Frattini p-loops

A p-loop Q is said to be *symplectic* if it possesses a central subloop F of order p such that $V = Q/F$ is an elementary Abelian p-group. Thus, by Theorem 2.1, Q is a symplectic p-loop if and only if $Q = V_\theta$ for a vector space V over $\mathbb{F}_p$ and a cocycle $\theta : V^2 \to \mathbb{F}_p$.

An element x of a loop Q is a *non-generator* if whenever $S \cup \{x\}$ generates Q then already S generates Q. Analogously to the situation in group theory, the *Frattini subloop* $\Phi(Q)$ of a loop Q consists of all non-generators of Q.

The Frattini subloop retains some (but not all) of the familiar properties of the Frattini subgroup. In particular, Bruck proved [2, pp. 97–99]: (i) $\Phi(Q)$ is the intersection of all maximal subloops of Q, (ii) if Q is nilpotent then $\Phi(Q)$ is a normal subloop of Q, (iii) if Q is a nilpotent p-loop then $\Phi(Q)$ is the least normal subloop of Q such that $Q/\Phi(Q)$ is an elementary Abelian p-group.

Following Hsu [17], we say that a p-loop Q is *small Frattini* if $|\Phi(Q)|$ divides p, and *central small Frattini* if it also satisfies $\Phi(Q) \le Z(Q)$.

As we have mentioned in the introduction, Hsu showed that even code loops are precisely small Frattini Moufang 2-loops. In addition, he showed that small Frattini Moufang p-loops are central small Frattini (and, importantly, that they are groups whenever $p > 3$). To generalize this result, let us have a look at nilpotent small Frattini p-loops:

Proposition 2.3 *Let Q be a p-loop. Then the following conditions are equivalent*:

(i) *Q is symplectic,*
(ii) *Q is nilpotent small Frattini,*
(iii) *Q is nilpotent central small Frattini.*

Proof Clearly, (iii) implies (ii). Assume that (ii) holds. If $|\Phi(Q)| = 1$ then Q is elementary Abelian and (i) follows. Suppose that $|\Phi(Q)| = p$, so $\Phi(Q) \cong \mathbb{Z}_p$. If Q is elementary Abelian, (i) holds. Else $1 < Q' = \Phi(Q)$, and thus $Q > Q' = Q_1 > Q_2 = 1 = Z_0(Q)$ is the lower central series. In particular, $Q_2 \le Z_0(Q)$, and so $Q' = Q_1 \le Z_1(Q) = Z(Q)$, proving (i).

Finally, assume (i), that is, there is $F \le Z(Q)$ such that $|F| = p$ and Q/F is elementary Abelian. Then $\Phi(Q) \le F$, and (iii) follows. □

By [12] and [13], Moufang p-loops are nilpotent. By [20], conjugacy closed p-loops are nilpotent. We therefore have:

Corollary 2.4 *Let Q be a small Frattini loop that is Moufang or conjugacy closed. Then Q is central small Frattini.*

Lemma 2.5 *Every two-element normal subloop is central.*

Proof Let $H = \{1, h\}$ be a normal subloop of Q. Since every inner mapping φ of Q fixes H globally and $\varphi(1) = 1$, we have $\varphi(h) = h$. But $Z(Q) = \{x \in Q;\ \varphi(x) = x$ for every inner mapping $\varphi\}$, so $H \le Z(Q)$ follows. □

Hence, a 2-loop Q is symplectic precisely when it possesses a normal subloop F of order 2 such that Q/F is an elementary Abelian group.

2.4 Conjugacy closed loops and symmetry of the associator mapping

Conditions relating the associator and commutator have been investigated already by Bruck [2], in an analogy to the commutator calculus of group theory. The condition

$$2[x,y]=[x,y,x-y] \tag{2.4}$$

is very natural for symplectic conjugacy closed p-loops, cf. Lemma 2.8, and it will play an important role in our investigation of code loops.

We start with a characterization of conjugacy closed loops in terms of associators and commutators, due to Kinyon, Kunen and Phillips:

Theorem 2.6 (Lemma 2.8 of [20]) *A loop Q is conjugacy closed if and only if the associator is a symmetric function of its arguments and all commutators are in the nucleus of Q.*

Since the commutators are in fact central in loops V_θ, by Lemma 2.2, we conclude that symplectic p-loops are conjugacy closed if and only if the associator mapping is symmetric.

Furthermore, by [7, Theorem 4.4 and Corollary 4.5], in any conjugacy closed loop of nilpotency class two we have $[u,v,w]=[uv,w][u,w]^{-1}[v,w]^{-1}$. Hence

$$A(u,v,w)=C(u+v,w)-C(u,w)-C(v,w) \tag{2.5}$$

holds in a symplectic p-loop with symmetric associator. This equation already hints at combinatorial polarization (see below).

For p odd, symplectic conjugacy closed p-loops were characterized by Drápal [8] by means of modifications of symplectic Abelian p-groups:

Theorem 2.7 (Theorem 7.1 of [8]) *Let p be an odd prime, and let $(G,+)$ be an Abelian group containing a subgroup F of order p such that $V=G/F$ is an elementary Abelian group. Let $f:V^3\to F$ be a symmetric trilinear form, and let $g:V^2\to F$ be an alternating bilinear form. Define a new multiplication $\circ$ on G by*

$$x\circ y=x+y+f(x+F,x+F,y+F)/2+g(x+F,y+F).$$

Then $(G,\circ)=G[f,g]$ is a symplectic conjugacy closed p-loop. Furthermore, every symplectic conjugacy closed p-loop is of the form $G[f,g]$ for some G, f, g as above.

The group $(G,+)$ from Theorem 2.7 is either an elementary Abelian p-group, or it is the direct product of an elementary Abelian p-group with the cyclic group of order p^2.

For a loop element x and an integer n, define the *left nth power* $x^{(n)}$ of x by $x^{(n)}=L_x^n(1)$. For instance, $x^{(4)}=x(x(xx))$.

Lemma 2.8 *Let p be an odd prime, and let G, F, $V = G/F$, f, g and $Q = G[f, g]$ be as in Theorem 2.7. Then*:

(i) $x^{(p)} = px$ *for every* $x \in Q$.
(ii) $(G, +)$ *is an elementary Abelian p-group if and only if* $x^{(p)} = 0$ *for every* $x \in Q$.
(iii) $[x, y, z] = f(x, y, z)$ *for every* $x, y, z \in Q$.
(iv) Q *satisfies* $2[x, y] = [x, y, x - y]$ *if and only if* $g = 0$.
(v) *If* $(G, +)$ *is elementary Abelian then* $Q = V_\theta$, *where* $\theta : V^2 \to F$ *is given by* $\theta(u, v) = f(u, u, v)/2 + g(u, v)$.

Proof Induction on k shows that the left translation L_x in Q satisfies

$$L_x^k(y) = kx + y + kh(x, y) + \binom{k}{2} h(x, x),$$

where $h(u, v) = f(u, u, v)/2 + g(u, v)$. In particular, $L_x^p(y) = px + y$ and $x^{(p)} = L_x^p(0) = px$, since $\mathrm{im}(h) \subseteq F$ and F is of odd order p. This proves (i) and (ii).

Since $g(x, y) + g(x + y, z) = g(y, z) + g(x, y + z)$, direct calculation yields

$$\begin{aligned}[x, y, z] &= (f(x, x, y) + f(x + y, x + y, z) - f(y, y, z) - f(x, x, y + z))/2 \\ &= f(x, y, z),\end{aligned}$$

proving (iii).

As $g(x, y) = -g(y, x)$, we have

$$\begin{aligned}[x, y] &= 2g(x, y) + (f(x, x, y) - f(y, y, x))/2 \\ &= 2g(x, y) + f(x, y, x - y)/2.\end{aligned}$$

Using this formula and (iii), we see that (2.4) holds if and only if $g = 0$, establishing (iv).

Assume that $(G, +)$ is an elementary Abelian p-group, i.e., $G = F \times V$. Since f, g are defined modulo F and their images are contained in F, the multiplication formula in $G[f, g]$ becomes

$$(a, u) \circ (b, v) = (a + b + f(u, u, v)/2 + g(u, v), u + v),$$

proving (v). □

2.5 Combinatorial polarization and n-applications

Combinatorial polarization has been introduced by Ward [31]. Proofs of all results mentioned in this subsection can be found either in [31] or in [9].

The notion of an n-application was developed by Ferrero and Micali [11] as a generalization of quadratic forms, which are precisely 2-applications. n-applications were studied (especially the question whether every n-application must be a polynomial mapping—the answer is "no") in a series of four papers by Prószyński [27]–[28].

Let V be a vector space over F, and $P : V \to F$ a mapping satisfying $P(0) = 0$. For $n \geq 1$, the *nth derived form* $\Delta_n P : V^n \to F$ of P is defined by

$$\Delta_n P(u_1, \dots, u_n) = \sum_{\{i_1,\dots,i_m\}\subseteq\{1,\dots,n\}} (-1)^{n-m} P(u_{i_1} + \cdots + u_{i_m}), \tag{2.6}$$

where the summation runs over all nonempty subset of $\{1, \dots, n\}$.

Then $\Delta_n P$ is clearly a symmetric form for every $n > 1$, and it is not hard to see that the defining identity (2.6) is equivalent to the recurrence relation

$$\begin{aligned}\Delta_n P(u, v, w_3, \dots, w_n)&\\ &= \Delta_{n-1} P(u + v, w_3, \dots, w_n)\\ &\quad - \Delta_{n-1} P(u, w_3, \dots, w_n) - \Delta_{n-1} P(v, w_3, \dots, w_n).\end{aligned} \tag{2.7}$$

We say that P has *combinatorial degree n* if $\Delta_n P \neq 0$ and $\Delta_{n+1} P = 0$. It is clear from (2.7) that P has combinatorial degree n if and only if $\Delta_n P \neq 0$ is a symmetric n-additive form. In particular, when F is a prime field, P has combinatorial degree n if and only if $\Delta_n P \neq 0$ is a symmetric n-linear form.

A mapping $P : V \to F$ is a *polynomial mapping* if with respect to some basis $\{e_1, \dots, e_n\}$ of V (and hence with respect to any basis of V) we have $P(\sum \lambda_i e_i) \in F[\lambda_1, \dots, \lambda_n]$. A polynomial mapping is said to be *reduced* if each of its exponents is smaller than $|F|$.

Recall that all algebras in this paper are finite. The Lagrange interpolation theorem therefore implies that every mapping $F \to F$ can be identified with a unique reduced polynomial over F, and an induction on the dimension of V shows that the same conclusion holds for every mapping $V \to F$, cf. [9].

By a result of [31], the combinatorial degree of a reduced polynomial mapping over $\mathbb{F}_p$ is equal to its polynomial degree. (The combinatorial degree of polynomial mappings can be easily calculated over any field, cf. [30] or [9].)

We say that $P : V \to F$ is an *n-application* if $\Delta_n P : V^n \to F$ is a symmetric n-linear form, and

$$P(\lambda u) = \lambda^n P(u)$$

for every $\lambda \in F$, $u \in V$.

We call a symmetric form $f : V^n \to F$ *characteristic*, a term we coined in [9], if $f(u_1, \dots, u_n) = 0$ whenever $u_{i_1} = \cdots = u_{i_p}$ for some $1 \leq i_1 < \cdots < i_p \leq n$, where $p = \mathrm{char}(F)$.

The following three theorems were obtained (more generally) in [9]:

Theorem 2.9 *Let V be a vector space over F, $n \geq 1$ and $P : V \to F$, $P(0) = 0$. Then $\Delta_n P : V^n \to F$ is a characteristic form.*

Theorem 2.10 *A reduced polynomial mapping $P : V \to F$ satisfies $P(\lambda u) = \lambda^n P(u)$ for every $\lambda \in F$, $u \in V$ if and only if the degree of every monomial of P is congruent to n modulo $|F| - 1$.*

Theorem 2.11 *Let $\{e_1, \dots, e_d\}$ be a basis of V over $\mathbb{F}_p$ and let $f : V^n \to \mathbb{F}_p$ be a characteristic n-linear form. Define $P : V \to \mathbb{F}_p$ by*

$$P\Big(\sum \lambda_i e_i\Big) = \sum_{0 \le t_i < p,\ t_1+\cdots+t_d=n} \frac{\lambda_1^{t_1} \cdots \lambda_d^{t_d}}{t_1! \cdots t_d!} f(t_1 * e_1, \dots, t_d * e_d),$$

where $t_i * e_i$ means that e_i is repeated as an argument of f precisely t_i times.

Then P is a reduced homogeneous polynomial of degree n (and hence an n-application) satisfying $\Delta_n P = f$.

Let us have a closer look at the case $n = 3$:

Proposition 2.12 *Let $\{e_1, \dots, e_d\}$ be a basis of V over $\mathbb{F}_p$ and let $f : V^3 \to \mathbb{F}_p$ be a characteristic trilinear form.*

(i) *If $p > 3$, there is a unique 3-application $P : V \to \mathbb{F}_p$ satisfying $\Delta_3 P = f$, namely*

$$P\Big(\sum \lambda_i e_i\Big) = \sum_{i<j<k} \lambda_i \lambda_j \lambda_k f(e_i, e_j, e_k) + \frac{1}{2} \sum_{i \ne j} \lambda_i^2 \lambda_j f(e_i, e_i, e_j) + \frac{1}{6} \sum_i \lambda_i^3 f(e_i, e_i, e_i).$$

(ii) *If $p = 3$, then $P : V \to \mathbb{F}_p$ defined by*

$$P\Big(\sum \lambda_i e_i\Big) = \sum_{i<j<k} \lambda_i \lambda_j \lambda_k f(e_i, e_j, e_k) + \frac{1}{2} \sum_{i \ne j} \lambda_i^2 \lambda_j f(e_i, e_i, e_j)$$

is a 3-application satisfying $\Delta_3 P = f$, and any other 3-application $R : V \to \mathbb{F}_p$ satisfying $\Delta_3 R = f$ differs from P by a linear polynomial.

(iii) *If $p = 2$, then $P : V \to \mathbb{F}_p$ defined by*

$$P\Big(\sum \lambda_i e_i\Big) = \sum_{i<j<k} \lambda_i \lambda_j \lambda_k f(e_i, e_j, e_k)$$

is a 3-application satisfying $\Delta_3 P = f$, and any other 3-application $R : V \to \mathbb{F}_p$ satisfying $\Delta_3 R = f$ differs from P by a quadratic polynomial.

Proof The three formulae are special cases of the general formula in Theorem 2.11, where we use the fact that $f(u, u, u) = 0$ when $p \le 3$ and $f(u, u, v) = 0$ when $p = 2$.

Assume that $R : V \to \mathbb{F}_p$ is another 3-application satisfying $\Delta_3 R = f$. By Theorem 2.10, every monomial of R has degree congruent to 3 modulo $p - 1$. Since $f = \Delta_3 R$ is trilinear, R has (combinatorial) degree at most 3.

Suppose that $p > 3$. It follows that every monomial of R has degree 3. Then R must coincide with P, else $R - P$ is a cubic polynomial, and so $0 = f - f = \Delta_3 R - \Delta_3 P = \Delta_3(R - P) \ne 0$, a contradiction.

Now suppose that $p = 3$. It follows that every monomial of R has degree 3 or 1, and we can argue as above that the cubic monomials of R and P coincide.

Similarly for $p = 2$. □

2.6 Linear codes and polarization

A *linear code*, often just a *code*, is a subspace of a vector space. Let $U \leq \mathbb{F}_p^n$ be a code. The *Hamming weight* $|u|$ of $u = (u_1, \dots, u_n) \in U$ is the number of nonzero coordinates u_i of u.

A binary code U is said to be of *level* r if 2^r divides $|u|$ for every $u \in U$. Binary codes of level 2 are known as *doubly even*. A code U is *self-orthogonal* if $\sum u_i v_i = 0$ for every $u, v \in U$.

Given two vectors u, v in $\mathbb{F}_2^n$, we denote by $u \cap v$ the vector w such that $w_i = 1$ if and only if $u_i = 1 = v_i$.

Here is the crucial link between binary vectors and polarization:

Lemma 2.13 (Lemma 11.8 of [1]) *Let U be a doubly even code and $P : U \to \mathbb{F}_2$ a mapping defined by $P(u) = |u|/4 \mod 2$. Then*

$$\Delta_2 P(u, v) = |u \cap v|/2 \mod 2,$$
$$\Delta_3 P(u, v, w) = |u \cap v \cap w| \mod 2$$

for every $u, v, w \in U$.

And here is the universality of binary codes with respect to polarization:

Theorem 2.14 (Theorem 3.2 of [30]) *Let V be a vector space over $\mathbb{F}_2$ and let $P : V \to \mathbb{F}_2$ be a mapping of combinatorial degree $r + 1$. Then there is a binary code U isomorphic to V (as a vector space) and of level r such that $P(u) = |u|/2^r \mod 2$ for every $u \in U$.*

In fact, we will only need a special case of Theorem 2.14 with $r = 2$, which has been established already in [3].

3 The definitions

We are now going to define code loops in four ways. The main result of this paper is to show that the four definitions are equivalent. Recall that $x^{(n)}$ stands for $L_x^n(1)$.

Definition 3.1 (Code loops via polarization) Let V be a vector space over $\mathbb{F}_p$, $\theta : V^2 \to \mathbb{F}_p$ a cocycle, and $Q = V_\theta$. Suppose that there is $P : V \to \mathbb{F}_p$ such that $A_\theta = \Delta_3 P$, $C_\theta(u, v) = \Delta_2 P(-u, v)$, and $P(\lambda u) = \lambda^3 P(u)$ for every $\lambda \in \mathbb{F}_p$ and u, $v \in V$. If $p \geq 3$, assume that $x^{(p)} = 1$ for every $x \in Q$. Then Q is a *code loop via polarization*.

Definition 3.2 (Code loops via code) Let U be a code over $\mathbb{F}_p$. If $p=2$, assume that U is doubly even. If $p=3$, assume that $\sum u_i = 0$ for every $u=(u_1,\dots,u_n)\in U$.

If $p=2$, let $\theta : U^2 \to \mathbb{F}_p$ be a cocycle satisfying

$$\theta(u,u) = \frac{|u|}{4} \mod 2,$$

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

$$\theta(u,v)+\theta(u+v,w)+\theta(v,w)+\theta(u,v+w) = |u\cap v\cap w| \mod 2$$

for every $u, v, w \in U$. If $p \geq 3$, define $\theta : U^2 \to \mathbb{F}_p$ by $\theta(u,v) = \sum u_i^2 v_i$.

Then $Q = U_\theta$ is a *code loop via code.*

Definition 3.3 (Code loops via conjugacy closed loop) Let Q be a symplectic conjugacy closed p-loop satisfying $2[x,y]=[x,y,x-y]$. If $p\geq 3$, assume that $x^{(p)}=1$ for every $x\in Q$. If $p=3$, assume also that $[x,x,x]=1$ for every $x\in Q$. Then Q is a *code loop via conjugacy closed loop.*

For odd primes we also define:

Definition 3.4 (Odd code loops via form) Let V be a vector space over $\mathbb{F}_p$, $p\geq 3$. Let $f : V^3 \to \mathbb{F}_p$ be a characteristic trilinear form, and let $\theta : V^2 \to \mathbb{F}_p$ be defined by $\theta(u,v) = f(u,u,v)/2$. Then $Q=V_\theta$ is an *odd code loop via form.*

4 Even code loops

Using existing literature, it is not difficult to establish the equivalence of the three definitions of even code loops. We present a short proof with several novel ideas, and we also show that even code loops can be characterized by seemingly weaker conditions.

Throughout this section, let $p=2$.

We start with an observation due to Aschbacher, cf. [1, Lemmas 12.11 and 12.18].

Lemma 4.1 *Let $Q=V_\theta$. Then $A(u,u,v)=0=A(u,v,v)$ holds if and only*

$$\theta(u,u+v)=\theta(u,u)+\theta(u,v), \textit{ and } \theta(u+v,v)=\theta(u,v)+\theta(v,v). \tag{4.1}$$

Moreover, when (4.1) holds then $C=\Delta_2 P$, where $P(u)=\theta(u,u)$.

Proof By Lemma 2.2, $A(u,u,v)=0=A(u,v,v)$ is equivalent to (4.1). Then

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

so

$$\begin{aligned}\theta(u+v,u+v) &= \theta(u+v,v)+\theta(u+v,u)\\ &= \theta(u,v)+\theta(v,v)+\theta(u,u)+\theta(v,u).\end{aligned} \tag{4.2}$$

Thus, with $P(u)=\theta(u,u)$, we have $\Delta_2 P(u,v)=\theta(u+v,u+v)+\theta(u,u)+\theta(v,v)=\theta(u,v)+\theta(v,u)=C(u,v)$, again by Lemma 2.2. □

The following result shows that the associator mapping is obtained by polarization under very weak assumptions:

Lemma 4.2 *Let $Q=V_\theta$ and assume that A satisfies $A(u,u,v)=A(u,v,v)=0$ and $A(u,v,w)=A(u,w,v)$ for every u, v, $w\in V$. Then $A=\Delta_3 P$, where $P(u)=\theta(u,u)$.*

Proof Let $P(u)=\theta(u,u)$. Then the equality $\Delta_3 P=A$ holds if and only if

$$\begin{aligned}&\theta(u,u)+\theta(v,v)+\theta(w,w)+\theta(u+v,u+v)+\theta(u+w,u+w)\\&\quad+\theta(v+w,v+w)+\theta(u+v+w,u+v+w)\\&\quad=\theta(u,v)+\theta(u+v,w)+\theta(v,w)+\theta(u,v+w).\end{aligned}\tag{4.3}$$

From (4.2), we have

$$\begin{aligned}\theta(u+v,u+v)&=\theta(u,u)+\theta(u,v)+\theta(v,u)+\theta(v,v),\\\theta(u+w,u+w)&=\theta(u,u)+\theta(u,w)+\theta(w,u)+\theta(w,w),\\\theta(u+v+w,u+v+w)&=\theta(u,u)+\theta(u,v+w)\\&\quad+\theta(v+w,u)+\theta(v+w,v+w).\end{aligned}$$

Upon substituting these three equalities into the left hand side of (4.3) and canceling as many summands as possible, we obtain

$$\theta(u,w)+\theta(v,u)+\theta(w,u)+\theta(v+w,u)=\theta(v,w)+\theta(u+v,w).$$

After adding $\theta(v,u+w)$ to both sides and rearranging, we get

$$\begin{aligned}&\theta(v,u)+\theta(v+u,w)+\theta(u,w)+\theta(v,u+w)\\&\quad=\theta(v,w)+\theta(v+w,u)+\theta(w,u)+\theta(v,u+w),\end{aligned}$$

which is merely $A(v,u,w)=A(v,w,u)$. □

Proposition 4.3 (Even code loops via polarization) *Let V be a vector space over $\mathbb{F}_2$ and let $\theta: V^2\to\mathbb{F}_2$ be a cocycle. The following conditions are equivalent for $Q=V_\theta$:*

(i) *Q is an even code loop via polarization, i.e., there is $P: V\to\mathbb{F}_2$ such that $P(0)=0$, $C=\Delta_2 P$, and $A=\Delta_3 P$.*
(ii) *$A=\Delta_3 P$, where $P(u)=\theta(u,u)$.*
(iii) *A satisfies $A(u,u,v)=A(u,v,v)=0$ and $A(u,v,w)=A(u,w,v)$.*
(iv) *A is a characteristic trilinear form.*
(v) *Q is Moufang.*
(vi) *Q is extra.*

Proof All derived forms are characteristic by Theorem 2.9, so (i) implies (iii). By Lemma 4.2, (iii) implies (ii). When (ii) holds then $C=\Delta_2 P$ by Lemma 4.1, and $P(0)=\theta(0,0)=0$, proving (i). Hence (i), (ii), (iii) are equivalent.

(v) is equivalent to (vi) since extra loops are precisely Moufang loops with squares in the nucleus, by [4, Corollary 2], and we have $(a,u)(a,u)=(\theta(u,u),0)\in Z(Q)$.

(ii) ⇔ (v): Recall that $\Delta_3 P(u,v,w)=\Delta_2 P(u+v,w)+\Delta_2 P(u,w)+\Delta_2 P(v,w)$, $C(u,v)=\theta(u,v)+\theta(v,u)$, and $A(u,v,w)=\theta(u,v)+\theta(u+v,w)+\theta(v,w)+\theta(u,v+w)$. When (ii) holds then $C=\Delta_2 P$ by Lemma 4.1, and so $\Delta_3 P=A$ is equivalent to $C(u+v,w)+C(u,w)+C(v,w)=A(u,v,w)$, which is

$$\theta(w,u+v)+\theta(u,w)+\theta(w,u)+\theta(w,v)=\theta(u,v)+\theta(u,v+w). \tag{4.4}$$

With $x=(a,u)$, $y=(c,w)$, $z=(b,v)$, the Moufang identity $x(y(xz))=((xy)x)z$ becomes

$$\begin{aligned}\theta(u,v)+\theta(w,u+v)+\theta(u,u+v+w)&\\ =\theta(u,w)+\theta(u+w,u)+\theta(w,v).&\end{aligned} \tag{4.5}$$

Now, Lemma 4.1 can be used whether (ii) or (v) is assumed, since Moufang loops are diassociative. We therefore have

$$\begin{aligned}\theta(u,u+v+w)&=\theta(u,u)+\theta(u,v+w),\\ \theta(u+w,u)&=\theta(u,u)+\theta(w,u)\end{aligned}$$

in either case, and these equations establish the equivalence of (4.4) and (4.5).

(v) ⇒ (iv): Assume that (v) holds. Then $A=\Delta_3 P$ with $P(u)=\theta(u,u)$, by (ii), and so A is a characteristic form. It remains to show that A is trilinear. By [2, Lemma VII.2.2], the right inner mapping $R(x,y)$ is a pseudoautomorphism with companion $[x,y]$. Since commutators are central in V_θ, $R(x,y)$ is an automorphism. Using centrality of associators, we also note that $R(x,y)t=(tx\cdot y)(xy)^{-1}=(t\cdot xy)(xy)^{-1}[t,x,y]=t[t,x,y]$, and so $(rs)[rs,x,y]=R(x,y)(rs)=R(x,y)r\cdot R(x,y)s=r[r,x,y]\cdot s[s,x,y]=(rs)[r,x,y][s,x,y]$. Upon canceling rs, we conclude that the associator mapping is trilinear.

Since (iv) trivially implies (iii), we are through. □

We are now ready for the characterization of even code loops:

Theorem 4.4 (Even code loops) *Definitions 3.1–3.3 of even code loops are equivalent.*

Proof Let $Q=U_\theta$ be an even code loop via code. By Lemma 2.13, $P:U\to\mathbb{F}_2$ defined by $P(u)=|u|/4 \mod 2$ satisfies $\Delta_2 P(u,v)=|u\cap v|/2 \mod 2$ and $\Delta_3 P(u,v,w)=|u\cap v\cap w| \mod 2$. By Lemma 2.2, we then have $C=\Delta_2 P$, $A=\Delta_3 P$, so Q is an even code loop via polarization.

Let $Q=V_\theta$ be an even code loop via polarization. Then the associator mapping is symmetric, commutators are in the nucleus, and hence Q is a symplectic conjugacy closed 2-loop by Theorem 2.6. Since Q is Moufang by Proposition 4.3, it is diassociative, and hence the condition (2.4) holds trivially. Thus Q is an even code loop via conjugacy closed loop.

Finally, assume that Q is an even code loop via conjugacy closed loop. Since Q is a symplectic 2-loop, $Q = V_\theta$ for some θ. By Theorem 2.6, A is symmetric. By (2.5), $A(u,u,v) = C(0,v) - C(u,v) - C(u,v) = 0$, so A is characteristic. Proposition 4.3 then implies that $A = \Delta_3 P$, $C = \Delta_2 P$, and $P(0) = 0$ for some $P : V \to \mathbb{F}_2$ of combinatorial degree at most 3. By [3] or by Theorem 2.14, there is a doubly even code U isomorphic to V such that $P(u) = |u|/4 \mod 2$. As above, we calculate $\Delta_2 P(u,v) = |u \cap v|/2 \mod 2$, $\Delta_3 P(u,v,w) = |u \cap v \cap w| \mod 2$, and so Q is an even code loop via code by Lemma 2.2. □

5 A universal code construction

In order to show the equivalence of Definitions 3.1–3.3 for even code loops, we needed Theorem 2.14 (with $r = 2$) to obtain doubly even codes with prescribed Hamming weights of codewords and their intersections. Theorem 5.6 below will play an analogous role in the odd case.

Lemma 5.1 *For $b_1, \dots, b_{p-1} \in \mathbb{F}_p$, the system of equations*

$$\begin{array}{ccccccccc} 1^1 a_1 & + & 2^1 a_2 & + & \cdots & + & (p-1)^1 a_{p-1} & = & b_1 \\ 1^2 a_1 & + & 2^2 a_2 & + & \cdots & + & (p-1)^2 a_{p-1} & = & b_2 \\ \vdots & & & & \ddots & & & & \vdots \\ 1^{p-1} a_1 & + & 2^{p-1} a_2 & + & \cdots & + & (p-1)^{p-1} a_{p-1} & = & b_{p-1} \end{array}$$

has a unique solution $a_1, \dots, a_{p-1} \in \mathbb{F}_p$.

Proof The determinant of the system is essentially a Vandermonde determinant,

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

$$= 1 \cdot 2 \cdots (p-1) \cdot \begin{vmatrix} 1 & 1 & \cdots & 1 \\ 1^1 & 2^1 & \cdots & (p-1)^1 \\ \vdots & & \ddots & \\ 1^{p-2} & 2^{p-2} & \cdots & (p-1)^{p-2} \end{vmatrix},$$

and thus is equal to $1 \cdot 2 \cdots (p-1) \cdot \prod_{0<i<j<p} (i-j) \not\equiv 0 \pmod{p}$. □

For a field F let $F^* = F \setminus \{0\}$ denote the multiplicative group of F.

Lemma 5.2 *Given $b_1, \dots, b_{p-1} \in \mathbb{F}_p$, there exists an $n \le (p-1)^2$ and $x_1, \dots, x_n \in \mathbb{F}_p^*$ such that*

$$\sum_{i=1}^{n} x_i^r = b_r \tag{5.1}$$

holds for every $1 \le r \le p-1$. Moreover, we can assume that each $i \in \mathbb{F}_p^*$ occurs less than p times among $x_1, \dots, x_n$, and under this assumption n is uniquely determined and $x_1, \dots, x_n$ are uniquely determined up to their order.

Proof Assume that $x_1, \dots, x_n$ satisfy (5.1) for every $1 \le r \le p-1$. Should some $i \in \mathbb{F}_p^*$ occur at least p times among $x_1, \dots, x_n$, we could delete p occurrences of i from $x_1, \dots, x_n$ without affecting the sums (5.1). We can therefore assume that each $i \in \mathbb{F}_p^*$ occurs among $x_1, \dots, x_n$ precisely a_i times, where $0 \le a_i < p$. Consequently, $n \le (p-1)^2$.

With a_i as above, the condition (5.1) is equivalent to

$$1^r a_1 + 2^r a_2 + \cdots + (p-1)^r a_{p-1} = b_r$$

for every $1 \le r \le p-1$, and we are done by Lemma 5.1. □

Let $A = (a_{ij})$ be an $n \times m$ matrix and B an $r \times s$ matrix. Let $A \otimes B$ be their *Kronecker product*, that is, the $nr \times ms$ block matrix

$$\begin{pmatrix} a_{11}B & \cdots & a_{1m}B \\ \vdots & \ddots & \vdots \\ a_{n1}B & \cdots & a_{nm}B \end{pmatrix}.$$

Denote by $A^{\otimes t}$ the Kronecker power $A \otimes \cdots \otimes A$, where A appears t times.

The following result is well known and easy to prove, cf. [22, 2.4.13]:

Lemma 5.3 *Let A be an $n \times n$ matrix and B an $m \times m$ matrix. Then $|A \otimes B| = |A|^m \cdot |B|^n$.*

Corollary 5.4 *Let A be an $n \times n$ matrix and $t \ge 1$. Then $|A^{\otimes t}| = |A|^{tn^{t-1}}$.*

Lemma 5.2 is a special case ($d = 1$) of this result:

Lemma 5.5 *Let $d \ge 1$, and for every $1 \le \lambda_1, \dots, \lambda_d \le p-1$ let $b_{\lambda_1,\dots,\lambda_d} \in \mathbb{F}_p$. Then there exists an $n \le (p-1)^{d+1}$ and $x_1 = (x_{1,i}), \dots, x_d = (x_{d,i}) \in (\mathbb{F}_p^*)^n$ such that*

$$\sum_{i=1}^{n} x_{1,i}^{\lambda_1} \cdots x_{d,i}^{\lambda_d} = b_{\lambda_1,\dots,\lambda_d} \tag{5.2}$$

for every $1 \le \lambda_1, \dots, \lambda_d \le p-1$. Moreover, we can assume that each d-tuple $(j_1, \dots, j_d) \in (\mathbb{F}_p^*)^d$ appears less than p times among $(x_{1,i}, \dots, x_{d,i})$, $1 \le i \le n$, *and under this assumption n is uniquely determined and* $x_1, \ldots, x_d$ *are uniquely determined up to a simultaneous permutation of coordinates* $1, \ldots, n$.

Proof Assume that $x_1, \ldots, x_d$ satisfy (5.2) for every $1 \le \lambda_1, \ldots, \lambda_d \le p-1$. Should some $j = (j_1, \ldots, j_d) \in (\mathbb{F}_p^*)^d$ occur at least p times among $(x_{1,i}, \ldots, x_{d,i})$, we could delete p corresponding coordinates from each x_k without affecting the sums (5.2). We can therefore assume that each $j \in (\mathbb{F}_p^*)^d$ occurs among $(x_{1,i}, \ldots, x_{d,i})$ precisely a_j times, where $0 \le a_j < p$. Consequently, $n \le (p-1)^{d+1}$.

Just as in the proof of Lemma 5.2, we can write down the system of $(p-1)^d$ linear equations in variables a_j. For $d = 2$, we get, with $r = p-1$,

$$\begin{array}{cccccccccc}
1^1 1^1 a_{1,1} & +\cdots+ & 1^1 r^1 a_{1,r} & +\cdots+ & r^1 1^1 a_{r,1} & +\cdots+ & r^1 r^1 a_{r,r} & = & b_{1,1} \\
 & \ddots & & \ddots & & \ddots & & & \vdots \\
1^1 1^r a_{1,1} & +\cdots+ & 1^1 r^r a_{1,r} & +\cdots+ & r^1 1^r a_{r,1} & +\cdots+ & r^1 r^r a_{r,r} & = & b_{1,r} \\
 & \ddots & & \ddots & & \ddots & & & \vdots \\
1^r 1^1 a_{1,1} & +\cdots+ & 1^r r^1 a_{1,r} & +\cdots+ & r^r 1^1 a_{r,1} & +\cdots+ & r^r r^1 a_{r,r} & = & b_{r,1} \\
 & \ddots & & \ddots & & \ddots & & & \vdots \\
1^r 1^r a_{1,1} & +\cdots+ & 1^r r^r a_{1,r} & +\cdots+ & r^r 1^r a_{r,1} & +\cdots+ & r^r r^r a_{r,r} & = & b_{r,r}.
\end{array}$$

The coefficients in the system correspond to the matrix $A \otimes A$, where

$$A = \begin{pmatrix} 1^1 & \cdots & r^1 \\ \vdots & \ddots & \vdots \\ 1^r & \cdots & r^r \end{pmatrix}.$$

For a general $d \ge 1$, it is now easy to see that we obtain a system with coefficient matrix $A^{\otimes d}$. We know from the proof of Lemma 5.1 that $|A| \not\equiv 0 \pmod{p}$, and thus $|A^{\otimes d}| \not\equiv 0 \pmod{p}$ by Corollary 5.4. □

Lemma 5.5 produces vectors $x_1, \ldots, x_d$ of optimal (shortest possible) length solving (5.2) for every $1 \le \lambda_1, \ldots, \lambda_d \le p-1$. We now allow $\lambda_i = 0$, too, but we do not claim anymore that the construction is optimal. While evaluating (5.2) with zero exponents, we adopt the convention $0^0 = 1$.

Theorem 5.6 (Universal code construction) *Let* $d \ge 1$, *and for every* $0 \le \lambda_1, \ldots, \lambda_d \le p-1$ *let* $b_{\lambda_1,\ldots,\lambda_d} \in \mathbb{F}_p$. *Then there exists an* $n > 0$ *and vectors* $x_1 = (x_{1,i}), \ldots, x_d = (x_{d,i}) \in \mathbb{F}_p^n$ *such that* (5.2) *holds for every* $0 \le \lambda_1, \ldots, \lambda_d \le p-1$. *It is possible to choose* $x_1, \ldots, x_d$ *so that they are linearly independent and hence generate a code of length n and dimension d.*

Proof We will build the vectors $x_1, \ldots, x_d$ inductively, starting with empty vectors $x_1, \ldots, x_d$, or with some linearly independent vectors $x_1, \ldots, x_d$, if linear independence is desired.

Given a subset I of $X = \{1, \ldots, d\}$, we say that (5.2) holds for I if it holds for every $0 \le \lambda_1, \ldots, \lambda_d \le p-1$ such that $\lambda_i \ne 0$ whenever $i \in I$. Given a subset $\mathcal{I}$ of the power set 2^X, we say that (5.2) holds for $\mathcal{I}$ if it holds for every $I \in \mathcal{I}$. Note that, for trivial reasons, (5.2) holds for $\mathcal{I} = \emptyset$.

For the inductive step, assume that (5.2) holds for some $\mathcal{I} \subseteq 2^X$. Further assume that $\mathcal{I}$ is an upset in 2^X with respect to inclusion, that is, if $I \in \mathcal{I}$ and $I \subseteq J \in 2^X$ then $J \in \mathcal{I}$. Let I be a maximal subset of X such that $I \notin \mathcal{I}$. We now extend the vectors $x_1, \dots, x_d$ so that (5.2) holds for the upset $\mathcal{I} \cup \{I\}$:

Extend all vectors x_i with $i \notin I$ by suitably many zeros. This will guarantee that (5.2) remains valid for $\mathcal{I}$, no matter how $\{x_i;\ i \in I\}$ will be extended later, since for every $J \in \mathcal{I}$ there is $i \in J \setminus I$. By Lemma 5.5, we can extend the vectors $\{x_i;\ i \in I\}$ so that (5.2) holds for I, too.

Starting with $\mathcal{I} = \emptyset$ and repeating the inductive step 2^d times in any suitable order (the first step will therefore be with $I = X$), we conclude that (5.2) holds for $\mathcal{I} = 2^X$. □

6 Odd code loops: Forms versus codes

In this section we show that odd code loops via forms are precisely odd code loops via codes.

Lemma 6.1 *Let $Q = U_\theta$ be an odd code loop via code. Then Q is an odd code loop via form.*

Proof Define $f : U^3 \to \mathbb{F}_p$ by $f(u, v, w) = 2\sum u_i v_i w_i$. Then $\theta(u, v) = \sum u_i^2 v_i = f(u, u, v)/2$. Moreover, f is clearly symmetric and trilinear. When $p = 3$, we have $f(u, u, u) = \sum u_i^3 = \sum u_i = 0$ by assumption on U, so f is characteristic. □

To prove the converse of Lemma 6.1, we need to construct a code from a characteristic trilinear form. The following easy lemma shows that it suffices to do this on a basis:

Lemma 6.2 *Let $Q = V_\theta$ be an odd code loop via form $f : V^3 \to \mathbb{F}_p$, with $\theta(u, v) = f(u, u, v)/2$. Let $\{e_1, \dots, e_d\}$ be a basis of V, and let $\varphi : V \to V'$, $e_j \mapsto x_j$ be an isomorphism of vector spaces. Assume that $f_{rst} = f(e_r, e_s, e_t) = \sum_i x_{r,i} x_{s,i} x_{t,i}$ for every $1 \le r \le s \le t \le d$. Then $\theta(u, v) = (1/2)\sum_i (\varphi(u)_i)^2 \varphi(v)_i$ for every $u, v \in V$.*

Proposition 6.3 *Odd code loops via forms are precisely odd code loops via codes.*

Proof In view of Lemma 6.1, it remains to show that odd code loops via forms are odd code loops via codes.

Let $Q = V_\theta$, f, $\{e_1, \dots, e_d\}$, f_{rst} be as in Lemma 6.2. By the same lemma, our task is to construct a basis $x_1, \dots, x_d$ of a code over $\mathbb{F}_p$ so that $f_{rst} = \sum_i x_{r,i} x_{s,i} x_{t,i}$ for every $1 \le r \le s \le t \le d$. In other words, we need to construct linearly independent vectors $x_1, \dots, x_d$ so that

$$
\begin{aligned}
&\sum_i x_{r,i}x_{s,i}x_{t,i} = f_{rst}, \quad \text{for } 1 \le r < s < t \le d,\\
&\sum_i x_{r,i}^2 x_{s,i} = f_{rrs}, \quad \sum_i x_{r,i}x_{s,i}^2 = f_{rss}, \quad \text{for } 1 \le r < s \le d, \\
&\sum_i x_{r,i}^3 = f_{rrr}, \quad \sum_i x_{r,i}^2 = 0, \quad \text{for } 1 \le r \le d.
\end{aligned}
\tag{6.1}
$$

When $p > 3$, this is immediately accomplished by Theorem 5.6. When $p = 3$, we have $\sum_i x_{r,i}^3 = \sum_i x_{r,i}$, and thus instead of $\sum_i x_{r,i}^3 = f_{rrr}$ we demand $\sum_i x_{r,i} = f_{rrr}$ in (6.1). So even when $p = 3$ we are done by Theorem 5.6, and the resulting code satisfies $\sum_i x_{r,i} = f_{rrr} = 0$, since f is characteristic. □

Note that we could construct a self-orthogonal code in the proof of Proposition 6.3, if needed, by imposing the additional condition $\sum_i x_{r,i}x_{s,i} = 0$ for $1 \le r < s \le d$.

6.1 Compatibility with Richardson's definition

In [29], Richardson defined odd code loops and suggested a generalization. Here is his definition:

Let U be a self-orthogonal code over $\mathbb{F}_p$, and let $z \in U$ be such that:

(i) all coordinates of z are nonzero,
(ii) z is invariant under all permutation matrices found in the automorphism group of U.

For $u, v \in U$, let $\theta(u, v) = \sum z_i^{-1} u_i^2 v_i$. Then $Q = (U, z) = U_\theta$ defined on $\mathbb{F}_p \times U$ by (2.1) is an *odd code loop in the sense of Richardson.*

Lemma 6.4 *Every odd code loop in the sense of Richardson is an odd code loop via form.*

Proof Let $Q = (U, z)$ be an odd code loop in the sense of Richardson. Consider $g : U^3 \to \mathbb{F}_p$, $g(u, v, w) = \sum z_i^{-1} u_i v_i w_i$. Then $\theta(u, v) = g(u, u, v)$, and g is symmetric trilinear. When $p = 3$, we have $g(u, u, u) = \sum_i z_i^{-1} u_i^3 = \sum_i z_i u_i = 0$, since U is self-orthogonal, and so g is characteristic. □

But not every odd code loop via form is an odd code loop in the sense of Richardson, as Example 6.5 shows.

Example 6.5 Let $F = \mathbb{F}_5$, α a generator of F^*, and V a 3-dimensional vector space over F with basis $\{e_1, e_2, e_3\}$. Let $f : V^3 \to F$ be the symmetric trilinear form defined by

$$
\begin{array}{lllll}
f_{111} = \alpha, & f_{112} = \alpha^3, & f_{113} = 0, & f_{122} = 0, & f_{123} = 0,\\
f_{133} = 1, & f_{222} = 1, & f_{223} = \alpha, & f_{233} = 0, & f_{333} = 1,
\end{array}
$$

where we write f_{ijk} instead of $f(e_i, e_j, e_k)$. Then one can verify (by computer) that f satisfies $f(v, v, v) \neq 0$ for every $0 \neq v \in V$.

Let $Q = V_\theta$, where $\theta(u, v) = f(u, u, v)/2$. Then Q is an odd code loop via form such that $A_\theta(v, v, v) = f(v, v, v) \neq 0$ for every $0 \neq v \in V$.

Let (U, z) be an odd code loop in the sense of Richardson, and let $g(u, v, w) = \sum z_i^{-1} u_i v_i w_i$. Then (U, z) is an odd code loop via form, and we therefore have $A(z, z, z) = g(z, z, z) = \sum z_i^2 = 0$ by Lemma 2.8 (iii). Hence Q is not isomorphic to (U, z).

On the other hand, Richardson suggested to generalize his definition to encompass all loops $Q = V_\theta$ with $\theta(u, v) = f(u, u, v)$, where $f : V^3 \to \mathbb{F}_p$ is symmetric trilinear. This generalization coincides with our definition via form when $p > 3$, but when $p = 3$ we impose the additional constraint $f(u, u, u) = 0$ for every u, i.e., we demand that f is characteristic. In view of Theorem 2.9, this constraint is necessary if we wish to maintain a connection to combinatorial polarization.

We conclude this section by showing that the special vector z in Richardson's definition is in fact not needed, since the all-1 vector can always take its place, possibly on account of a longer self-orthogonal code.

Recall that the *radical* of a symmetric trilinear form $f : V^3 \to \mathbb{F}_p$ is the subspace $\mathrm{Rad}(f) = \{u \in V;\ f(u, v, w) = 0 \text{ for every } v, w \in V\}$. In Richardon's definition, the codeword z belongs to the radical of the associated form $g(u, v, w) = \sum z_i^{-1} u_i v_i w_i$. Indeed, $g(z, u, v) = \sum u_i v_i = 0$ thanks to self-orthogonality.

Lemma 6.6 *Let V be a self-orthogonal code with basis $\{e_1, \dots, e_{d+1}\}$, $f : V^3 \to \mathbb{F}_p$ a characteristic trilinear form, and $z \in V \cap \mathrm{Rad}(f)$. Then there is a self-orthogonal code V' containing the all-1 vector $\mathbf{1}$, and there is an isomorphism $\varphi : V \to V'$ such that $\varphi(z) = \mathbf{1}$, $\varphi(e_i) = x_i$ for every i, and $\sum_i x_{r,i} x_{s,i} x_{t,i} = f(e_r, e_s, e_t)$ for every $1 \leq r, s, t \leq d + 1$.*

Proof Without loss of generality, let $z = e_{d+1}$. We need to construct linearly independent vectors $x_1, \dots, x_{d+1}$ generating a self-orthogonal code such that (6.1) holds *and* $x_{d+1} = \mathbf{1}$. By Theorem 5.6, there exist vectors $x_1, \dots, x_d$ satisfying (6.1), $\sum_i x_{r,i} x_{s,i} = 0$ for every $1 \leq r < s \leq d$, and $\sum_i x_{r,i} = 0$ for every $1 \leq r \leq d$. (When $p = 3$ we use the assumption $f_{rrr} = 0$.)

Having $x_{d+1} = \mathbf{1}$ imposes additional conditions on the vectors $x_1, \dots, x_d$. Namely, the first equation of (6.1) yields $\sum_i x_{r,i} x_{s,i} = f_{rs(d+1)} = 0$ (which already holds), the second yields $\sum_i x_{r,i}^2 = f_{rr(d+1)} = 0$ (which already holds), the third yields $\sum_i x_{r,i} = f_{r(d+1)(d+1)} = 0$ (which already holds), the fourth yields $\sum_i x_{d+1,i}^3 = f_{(d+1)(d+1)(d+1)} = 0$, and the fifth equation of (6.1) yields $\sum_i x_{d+1,i}^2 = 0$. To make x_{d+1} orthogonal to all other basis vectors, we must have $\sum x_{r,i} = 0$ for every $1 \leq r \leq d$ (which already holds). To make x_{d+1} self-orthogonal, we demand $\sum_i x_{d+1,i} = 0$. We accomplish $\sum_i x_{d+1,i} = \sum_i x_{d+1,i}^2 = \sum_i x_{d+1,i}^3 = 0$ at once by extending $x_1, \dots, x_d$ by suitably many zeros so that the length of V' is divisible by p. □

7 Odd code loops: Forms versus polarization

Lemma 7.1 *Let $p \geq 3$, and let $Q = V_\theta$ be such that the associator map A is a characteristic trilinear form. Let P be the unique homogeneous cubic polynomial $V \to \mathbb{F}_p$ satisfying $\Delta_3 P = A$. Then $A(u,u,u) = C(2u,u) = 6P(u)$ and $2\Delta_2 P(-u,v) = A(u,v,u-v)$ holds for every $u, v \in V$.*

Proof The existence and uniqueness of P follow from Proposition 2.12. We have

$$A(u,u,u) = \theta(u,u) + \theta(2u,u) - \theta(u,u) - \theta(u,2u) = C(2u,u),$$

by Lemma 2.2, and

$$\begin{aligned} A(u,u,u) &= \Delta_3 P(u,u,u) = P(3u) - 3P(2u) + 3P(u) \\ &= (27 - 3 \cdot 8 + 3)P(u) = 6P(u) \end{aligned}$$

since P is homogeneous and cubic.

Let $p > 3$. The equality $2\Delta_2 P(-u,v) = A(u,v,u-v)$ holds if and only if

$$\begin{aligned} 2\Delta_2 P(-u,v) &= \Delta_3 P(u,v,u-v) \\ &= \Delta_2 P(u+v,u-v) - \Delta_2 P(u,u-v) - \Delta_2 P(v,u-v), \end{aligned}$$

which holds if and only if

$$\begin{aligned} &2P(-u+v) - 2P(-u) - 2P(v) \\ &\quad = P(2u) - P(u+v) - P(u-v) - P(2u-v) \\ &\qquad + P(u) + P(u-v) - P(u) + P(v) + P(u-v) \\ &\quad = P(2u) - P(u+v) - P(2u-v) + P(u-v) + P(v). \end{aligned}$$

Using $P(\lambda u) = \lambda^3 P(u)$ again, the above equality is equivalent to

$$3P(-u+v) - 3P(v) - 6P(u) + P(u+v) + P(2u-v) = 0. \tag{7.1}$$

Using $A(u,u,u) = 6P(u)$ and the symmetry and trilinearity of A, we have

$$\begin{aligned} 3P(-u+v) &= (3/6)(-A(u,u,u) + 3A(u,u,v) - 3A(u,v,v) + A(v,v,v)), \\ -3P(v) &= (-3/6)A(v,v,v), \\ -6P(u) &= (-6/6)A(u,u,u), \\ P(u+v) &= (1/6)(A(u,u,u) + 3A(u,u,v) + 3A(u,v,v) + A(v,v,v)), \\ P(2u-v) &= (1/6)(8A(u,u,u) - 12A(u,u,v) + 6A(u,v,v) - A(v,v,v)), \end{aligned}$$

so (7.1) holds.

Let $p=3$ and $u=\sum\lambda_i e_i$, $v=\sum\mu_i e_i$. By Proposition 2.12 (ii) and $P(-u)=-P(u)$, we have

$$\begin{aligned}2\Delta_2P(-u,v)&=2(P(v-u)+P(u)-P(v))\\&=\sum_{i\neq j}A(e_i,e_i,e_j)[(\mu_i-\lambda_i)^2(\mu_j-\lambda_j)+\lambda_i^2\lambda_j-\mu_i^2\mu_j]\\&\quad+2\sum_{i<j<k}A(e_i,e_j,e_k)[(\mu_i-\lambda_i)(\mu_j-\lambda_j)(\mu_k-\lambda_k)\\&\quad+\lambda_i\lambda_j\lambda_k-\mu_i\mu_j\mu_k].\end{aligned}$$

On the other hand, since $A(w,w,w)=6P(w)=0$, we have

$$\begin{aligned}A(u,v,u-v)&=\sum_{i,j,k}\lambda_i\mu_j(\lambda_k-\mu_k)A(e_i,e_j,e_k)\\&=\sum_{i\neq j}A(e_i,e_i,e_j)[\lambda_i\mu_i(\lambda_j-\mu_j)\\&\quad+\lambda_i\mu_j(\lambda_i-\mu_i)+\lambda_j\mu_i(\lambda_i-\mu_i)]\\&\quad+\sum_{i<j<k}A(e_i,e_j,e_k)[\lambda_i\mu_j(\lambda_k-\mu_k)\\&\quad+\lambda_i\mu_k(\lambda_j-\mu_j)+\lambda_j\mu_i(\lambda_k-\mu_k)\\&\quad+\lambda_j\mu_k(\lambda_i-\mu_i)+\lambda_k\mu_i(\lambda_j-\mu_j)+\lambda_k\mu_j(\lambda_i-\mu_i)].\end{aligned}$$

A tedious comparison of the coefficients of $A(e_i,e_i,e_j)$ and $A(e_i,e_j,e_k)$ in the two expressions then yields $2\Delta_2P(-u,v)=A(u,v,u-v)$. □

Lemma 7.2 *Every odd code loop via form is an odd code loop via polarization.*

Proof Assume that $Q=V_\theta$ is an odd code loop via form f, $\theta(u,v)=f(u,u,v)/2$. By Lemma 2.8(ii), $x^{(p)}=1$ for every $x\in Q$. Using Lemma 2.8(iii) with $g=0$, we get $A=f$. By Lemma 7.1, there is a (unique) homogeneous cubic polynomial $P:V\to\mathbb{F}_p$ such that $\Delta_3P=A$. We therefore have $P(\lambda u)=\lambda^3P(u)$, so it remains to show that $C(u,v)=\Delta_2P(-u,v)$, which by Lemma 7.1 is equivalent to $2C(u,v)=A(u,v,u-v)$. But we have $2C(u,v)=2\theta(u,v)-2\theta(v,u)=f(u,u,v)-f(v,v,u)=f(u,v,u-v)=A(u,v,u-v)$. □

Proposition 7.3 *Odd code loops via form are precisely odd code loops via polarization.*

Proof It remains to show that an odd code loop $Q=V_\theta$ via polarization of $P: V\to\mathbb{F}_p$ is an odd code loop via form.

Since $A=\Delta_3P$ is symmetric, Theorem 2.6 implies that Q is a symplectic conjugacy closed p-loop. By Theorem 2.7, $Q=G[f,g]$ for some Abelian group

$(G,+)$, symmetric trilinear form f and an alternating bilinear form g. By Lemma 2.8(iii), $f=A=\Delta_3 P$ is characteristic trilinear, so P is a 3-application. By Proposition 2.12, there is a homogeneous cubic polynomial $R: V\to\mathbb{F}_p$ that differs from P by a linear polynomial. Hence $\Delta_3 P=\Delta_3 R$, $\Delta_2 P=\Delta_2 R$, and Lemma 7.1 yields $2\Delta_2 P(-u,v)=2\Delta_2 R(-u,v)=A(u,v,u-v)$. We have $C(u,v)=\Delta_2 P(-u,v)$ by assumption, and so $2C(u,v)=A(u,v,u-v)$. Lemma 2.8(iv) then implies that $g=0$. Since $x^{(p)}=1$ for every $x\in Q$, $(G,+)$ is elementary Abelian by Lemma 2.8(ii), and we are done by Lemma 2.8(v). □

8 Odd code loops: Forms versus conjugacy closed loops

Proposition 8.1 *Odd code loops via form are precisely odd code loops via conjugacy closed loop.*

Proof When $Q=V_\theta$ is an odd code loop via form f, we can view it as the loop $G[f,0]$ of Theorem 2.7, where $(G,+)=(\mathbb{F}_p\times U,+)$ is elementary Abelian. By Lemma 2.8, $x^{(p)}=1$ for every $x\in Q$, and (2.4) holds. When $p=3$, $A(x,x,x)=f(x,x,x)=0$. Hence Q is a code loop via conjugacy closed loop.

Conversely, let Q be an odd code loop via conjugacy closed loop. By Theorem 2.7 and Lemma 2.8, we can assume that $Q=V_\theta$ where $\theta(u,v)=f(u,u,v)/2+g(u,v)$, f is symmetric trilinear and g is alternating bilinear. The assumption $[x,x,x]=1$ then guarantees that $A=f$ is characteristic even when $p=3$, and since (2.4) holds, we have $g=0$ by Lemma 2.8. Thus Q is a code loop via form f. □

In summary:

Theorem 8.2 (Odd code loops) *The four definitions 3.1–3.4 of odd code loops are equivalent.*

9 Some basic properties of odd code loops

The properties of odd code loops established by Richardson in [29, pp. 1468–9] remain valid for our odd code loops. In fact, Richardson's proofs can be used almost verbatim, accounting merely for a change in notation. We restate them here for the sake of completeness.

An element of a loop is *power-associative* if it generates an associative subloop, i.e., a group. A loop is *power-associative* if each of its elements is power-associative.

Lemma 9.1 *Let $V_\theta=F\times V$ be a loop such that $A(au,bv,cw)=abcA(u,v,w)$ for every a, b, $c\in F$ and u, v, $w\in V$. Then $x\in V_\theta$ is power-associative if and only if $A(x,x,x)=0$.*

Proof If x is power-associative then certainly $A(x,x,x)=0$. Conversely, assume that $A(u,u,u)=0$ for some $x=(a,u)\in V$. Since $(a,u)(b,v)=(a+b+$

$\theta(u,v), u+v)$, any element in the subloop generated by x is of the form (a_1, a_2u), where $a_1, a_2 \in F$. Now, $A(a_2u, b_2u, c_2u) = a_2b_2c_2A(u,u,u) = 0$ for every a_2, b_2, $c_2 \in F$ by our assumption, and so x is power-associative. □

Corollary 9.2 *When $p = 3$, odd code loops are power-associative.*

Proof Consider an odd code loop via form f. Then $A = f$ is characteristic, and we are done by Lemma 9.1. □

Lemma 9.3 *An odd code loop is commutative if and only if it is an elementary Abelian p-group.*

Proof Let $Q = V_\theta$ be an odd code loop via form f. The commutator and associator mappings are related according to (2.4). Thus, if Q is associative, it is commutative. Conversely, assume that Q is commutative. Then $2\theta(u,-v) = A(u,u,-v) = -A(u,u,v) = -2\theta(u,v) = -2\theta(v,u) = -2A(v,v,u) = -2A(-v,-v,u) = -2\theta(-v,u) = -2\theta(u,-v)$, so $\theta(u,-v) = 0$ for every $u, v \in V$. □

Corollary 9.4 *Assume that $p > 3$. Then an odd code loop is power-associative if and only if it is an elementary Abelian p-group.*

Proof Let $Q = V_\theta$ be a power-associative odd code loop. Then $0 = A(u-v, u-v, u-v) = A(u,u,u) + 3A(u,v,v) - 3A(u,u,v) - A(v,v,v) = -3A(u,v,u) - 3A(u,v,-v) = -6C(u,v)$ by (2.4). Hence Q is an elementary Abelian p-group by Lemma 9.3. □

We conclude this section with a solution to the isomorphism problem for code loops:

Theorem 9.5 (Theorem 12.17 of [1]) *Let V_θ, V_ϑ be even code loops. Then V_θ is isomorphic to V_ϑ if and only if $(P_\theta, C_\theta, A_\theta)$ is conjugate to $(P_\vartheta, C_\vartheta, A_\vartheta)$ under $GL(V)$, that is, there is $\varphi \in GL(V)$ such that $P_\theta(u) = P_\vartheta(\varphi u)$, $C_\theta(u,v) = C_\vartheta(\varphi u, \varphi v)$, and $A_\theta(u,v,w) = A_\vartheta(\varphi u, \varphi v, \varphi w)$ for every $u, v, w \in V$.*

Theorem 9.6 (Theorem 7.2 of [8]) *Let V_{θ_1}, V_{θ_2} be odd code loops via characteristic trilinear forms f_1, $f_2 : V^3 \to \mathbb{F}_p$, respectively. Then there exists an isomorphism $V_{\theta_1} \to V_{\theta_2}$ that maps $\mathbb{F}_p \times 0$ onto $\mathbb{F}_p \times 0$ if and only if f_1, f_2 are similar, that is, there is $\varphi \in GL(V)$ such that $f_1(u,v,w) = f_2(\varphi u, \varphi v, \varphi w)$ for every $u, v, w \in V$.*

10 Concluding remarks

10.1 Realizing characteristic trilinear forms as associators of code loops

When p is odd, every characteristic trilinear form $V^3 \to \mathbb{F}_p$ can be trivially realized as the associator of an odd code loop, by Definition 3.4. An analogous result is true for $p = 2$:

Proposition 10.1 *Let V be a vector space over $\mathbb{F}_p$, $\theta : V^2 \to \mathbb{F}_p$ a cocycle, and V_θ a code loop. Then A_θ is a characteristic trilinear form.*

Conversely, given a characteristic trilinear form $f : V^3 \to \mathbb{F}_p$, there is a cocycle $\theta : V^2 \to \mathbb{F}_p$ such that $Q = V_\theta$ is a code loop and $A_\theta = f$. When $p > 2$, it suffices to take $\theta(u, v) = f(u, u, v)/2$. When $p = 2$, it suffices to take

$$\theta\Big(\sum \lambda_i e_i, \sum \mu_k e_k\Big) = \sum_{i<j} \lambda_i \lambda_j \mu_k f(e_i, e_j, e_k), \tag{10.1}$$

where $\{e_1, \ldots, e_d\}$ is a basis of V.

Proof There is nothing to show in the odd case.

When V_θ is an even code loop then A_θ is a characteristic trilinear form by Proposition 4.3. Conversely, let $f : V^3 \to \mathbb{F}_2$ be a characteristic trilinear form, and let θ be defined as in (10.1). Then

$$\theta\Big(\sum \lambda_i e_i, \sum \mu_j e_j\Big) = \sum_{i<j<k} (\lambda_i \lambda_j \mu_k + \lambda_i \lambda_k \mu_j + \lambda_j \lambda_k \mu_i) f(e_i, e_j, e_k). \tag{10.2}$$

With $u = \sum \lambda_i e_i$, $v = \sum \mu_j e_j$, $w = \sum \nu_k e_k$, we have

$$\begin{aligned} A_\theta(u, v, w) &= \theta(u, v) + \theta(u + v, w) + \theta(v, w) + \theta(u, v + w) \\ &= \sum_{i<j<k} c_{ijk} f(e_i, e_j, e_k), \end{aligned}$$

where

$$\begin{aligned} c_{ijk} &= \lambda_i \lambda_j \mu_k + \lambda_i \lambda_k \mu_j + \lambda_j \lambda_k \mu_i \\ &\quad + (\lambda_i + \mu_i)(\lambda_j + \mu_j)\nu_k + (\lambda_i + \mu_i)(\lambda_k + \mu_k)\nu_j \\ &\quad + (\lambda_j + \mu_j)(\lambda_k + \mu_k)\nu_i \\ &\quad + \mu_i \mu_j \nu_k + \mu_i \mu_k \nu_j + \mu_j \mu_k \nu_i \\ &\quad + \lambda_i \lambda_j (\mu_k + \nu_k) + \lambda_i \lambda_k (\mu_j + \nu_j) + \lambda_j \lambda_k (\mu_i + \nu_i) \\ &= \lambda_i \mu_j \nu_k + \mu_i \lambda_j \mu_k + \lambda_i \mu_k \nu_j + \mu_i \lambda_k \nu_j + \lambda_j \mu_k \nu_i + \mu_j \lambda_k \nu_i \\ &= \sum_{i \neq j \neq k \neq i} \lambda_i \mu_j \nu_k. \end{aligned}$$

Since $f(u, u, v) = 0$, we conclude that $A_\theta = f$. Then V_θ is an even code loop, by Proposition 4.3. □

The somewhat mysterious formula (10.1) is an interpretation of $f(u, u, v)/2$ over $\mathbb{F}_2$. Indeed, take a characteristic trilinear form $f : V^3 \to \mathbb{F}_2$, and note that

$$\begin{aligned} &f\Bigl(\sum \lambda_i e_i, \sum \lambda_j e_j, \sum \mu_k e_k\Bigr) \\ &\quad = 2\sum_{i<j} \lambda_i\lambda_j\mu_k f(e_i,e_j,e_k) + \sum \lambda_i^2\mu_j f(e_i,e_i,e_j) = 2\sum_{i<j}\lambda_i\lambda_j\mu_k f(e_i,e_j,e_k) \end{aligned}$$

with respect to some basis $\{e_1,\dots,e_d\}$ of V.

It is therefore not unreasonable to say that a characteristic trilinear form f can be realized as an associator A_θ of a code loop by setting $\theta(u,v)$ equal to "half of $f(u,u,v)$" in both the odd and even cases.

10.2 The mapping P

When $p=2$, Definition 3.1 reduces to $A=\Delta_3 P$, $C=\Delta_2 P$, and $P(0)=0$. But Proposition 4.3(iii) shows that seemingly much weaker conditions are sufficient. Roughly speaking, the condition $A(u,u,v)=0=A(u,v,v)$ forces the loop Q to be diassociative, while $A(u,v,w)=A(u,w,v)$ implies that A is a symmetric function, and thus that Q is a conjugacy closed loop. In particular, the polarization relations are obtained for free.

Our results imply that the mapping P satisfies $\Delta_4 P=0$ for every p, which is certainly not obvious from Definition 3.1.

An interesting question is how much freedom do we have in choosing P in Definition 3.1 for a given code loop V_θ.

When $p>3$, P is uniquely determined already by the condition $\Delta_3 P=A$, by Proposition 2.12. (This also means that the unpleasant sign change in $C(u,v)=\Delta_2 P(-u,v)$ cannot be disposed of.) Moreover, if $f: V^3\to\mathbb{F}_p$ is a characteristic trilinear form such that $\theta(u,v)=f(u,u,v)/2$, we have

$$P(u)=A(u,u,u)/6=f(u,u,u)/6=\theta(u,u)/3,$$

by Lemma 7.1.

When $p=2$, P is determined up to a linear polynomial with zero constant term (since $\Delta_3 P=A$, $\Delta_2 P=C$, and $P(0)=0$ is assumed). Moreover, it is possible to choose P as $P(u)=\theta(u,u)(=\theta(u,u)/3)$, by Proposition 4.3. With this choice, $P(u)=\theta(u,u)$ is the squaring map, as $(a,u)(a,u)=(\theta(u,u),0)$ holds in an even code loop V_θ.

When $p=3$, P is determined up to a linear polynomial R satisfying $R(\lambda u)=\lambda^3 R(u)$ already by the condition $\Delta_3 P=A$, by Proposition 2.12. Moreover, unless $P=0$, there is no $a\in\mathbb{F}_3^*$ for which $P(u)=a\theta(u,u)$ works, since $\theta(u,u)=f(u,u,u)/2=0$.

10.3 Weak forms of associativity

It is a coincidence that symplectic conjugacy closed 2-loops are precisely symplectic Moufang 2-loops. One of the messages of this paper is that the investigation of code loops should follow the trail of conjugacy closed loops, not Moufang loops.

The condition (2.4) of Definition 3.3 holds automatically when $p=2$, since even code loops are diassociative.

Power-associativity of odd code loops for $p=3$ is an artifact of combinatorial polarization, and it has to be explicitly enforced in Definitions 3.2–3.4 (by the assumptions $\sum u_i = 0$, $[x,x,x]=1$, and f is characteristic, respectively). It is perhaps not obvious that the condition $[x,x,x]=1$ is independent of the remaining assumptions in Definition 3.3, but the following example shows that it is:

Example 10.2 Let V be a vector space over $\mathbb{F}_3$ with basis $\{e_1,e_2\}$. Let $f: V^3 \to \mathbb{F}_3$ be the symmetric trilinear form defined by $f(e_i,e_j,e_k)=0$ for every $1 \le i,j,k \le 2$, except for $f(e_2,e_2,e_2)=1$. Let $(G,+)$ be the elementary Abelian 3-group $\mathbb{F}_3 \times V$, and let $Q = G[f,0]$ be as in Theorem 2.7. Then by Theorem 2.7 and Lemma 2.8, Q is a symplectic conjugacy closed 3-loop in which (2.4) holds and $x^{(3)}=1$ for every $x \in Q$, but $[x,x,x]=f(x,x,x)$ does not vanish for some $x \in Q$.

Finally, let us have a look at the condition

$$x^{(p)} = 1 \tag{10.3}$$

from Definitions 3.1, 3.3.

We claim that if (10.3) holds in a code loop Q then the seemingly stronger condition $L_x^p(y)=y$ holds as well. For $p=2$, this is obvious from diassociativity of Q. When $p \ge 3$, note that the proof of Lemma 2.8 in fact shows not only that $(G,+)$ is elementary Abelian precisely when (10.3) holds, but also that $(G,+)$ is elementary Abelian precisely when $L_x^p(y)=y$.

We remark that (10.3) must be dropped from Definitions 3.1, 3.3 for $p=2$, else we would only obtain elementary Abelian 2-groups, by Proposition 4.3.

The following example shows that (10.3) is independent of the remaining conditions in Definition 3.1:

Example 10.3 As in [7], let $(Q,*)$ be defined on $\mathbb{Z}_{25}$ by $x*y = x+y+5x^2y$. Then Q is a symplectic conjugacy closed loop in which $x^{(5)}=1$ does not hold for all $x \in Q$. But the mapping $P: \mathbb{Z}_5 \to \mathbb{Z}_5$, $x \mapsto 2x^3$ satisfies $P(\lambda u) = \lambda^3 P(u)$, $\Delta_3 P = A$, and $C(-u,v) = \Delta_2 P(u,v)$ for every $u, v \in \mathbb{Z}_5$.

Lastly, the condition (10.3) on left powers can in code loops be replaced by the condition $R_x^p(1)=1$ on right powers. Indeed, induction on k in $G[f,g]$ yields

$$\begin{aligned} R_x^k(y) &= y + kx + g(y,x)k + g(x,x)k(k-1)/2 \\ &\quad + f(y,y,x)k/2 + f(y,x,x)(k-1)k/2 \\ &\quad + f(x,x,x)(k-1)k(2k-1)/12, \end{aligned}$$

and thus $R_x^p(y) = y + px + f(x,x,x)(p-1)p(2p-1)/12$. Since p divides $(p-1)p(2p-1)/12$ when $p>3$, we get $R_x^p(y) = px + y$ for $p>3$, and we see that $R_x^p(0)=0$ holds if and only if $(G,+)$ is an elementary Abelian p-group. When $p=3$, we are done by Corollary 9.2.

However, there exists a symplectic conjugacy closed 3-loop of order 9 in which $x(xx)=1$ holds but $(xx)x=1$ does not. To see what happens when (10.3) is dropped from Definition 3.3, see [8].

References

1. Aschbacher, M.: Sporadic Groups. Cambridge Tracts in Mathematics, vol. 104. Cambridge University Press, Cambridge (1994)
2. Bruck, R.H.: A Survey of Binary Systems, third printing, corrected. Ergebnisse der Mathematik und Ihrer Grenzgebiete, New Series, vol. 20. Springer, Berlin (1971)
3. Chein, O., Goodaire, E.G.: Moufang loops with a unique nonidentity commutator (associator, square). J. Algebra **130**, 369–384 (1990)
4. Chein, O., Robinson, D.A.: An "extra" law for characterizing Moufang loops. Proc. Amer. Math. Soc. **33**, 29–32 (1972)
5. Conway, J.H.: A simple construction for the Fischer-Griess Monster group. Invent. Math. **79**, 513–540 (1985)
6. Conway, J.H., Sloane, N.J.A.: Sphere Packings, Lattices and Groups, third edition. Grundlehren der mathematischen Wissenschaften, vol. 290. Springer, Berlin (1999)
7. Csörgő, P., Drápal, A.: Left conjugacy closed loops of nilpotency class two. Results Math. **47**(3–4), 242–265 (2005)
8. Drápal, A.: On extraspecial left conjugacy closed loops. J. Algebra **302**, 771–792 (2006)
9. Drápal, A., Vojtěchovský, P.: Symmetric multilinear forms and polarization of polynomials. Linear Algebra Appl. **431**, 998–1012 (2009)
10. Eilenberg, S., MacLane, S.: Algebraic cohomology groups and loops. Duke Math. J. **14**, 435–463 (1947)
11. Ferrero, M., Micali, A.: Sur les n-applications. Coll. Formes Quadratiques 2 (Montpellier, 1977), Bull. Soc. Math. France Mém. No. **59**, 33–53 (1979)
12. Glauberman, G.: On loops of odd order II. J. Algebra **8**, 393–414 (1968)
13. Glauberman, G., Wright, C.R.B.: Nilpotence of finite Moufang 2-loops. J. Algebra **8**, 415–417 (1968)
14. Griess, R.L. Jr.: A construction of F_1 as automorphisms of a 196, 883-dimensional algebra. Proc. Nat. Acad. Sci. **78**, 689–691 (1981)
15. Griess, R.L. Jr.: The friendly giant. Invent. Math. **69**, 1–102 (1982)
16. Griess, R.L. Jr.: Code loops. J. Algebra **100**, 224–234 (1986)
17. Hsu, T.: Moufang loops of class 2 and cubic forms. Math. Proc. Cambridge Philos. Soc. **128**(2), 197–222 (2000)
18. Hsu, T.: Explicit constructions of code loops as centrally twisted products. Math. Proc. Cambridge Philos. Soc. **128**(2), 223–232 (2000)
19. Johnson, K.W., Leedham-Green, C.R.: Loop cohomology. Czechoslovak Math. J. **40**(115(2)), 182–194 (1990)
20. Kinyon, M.K., Kunen, K.: Power-associative, conjugacy closed loops. J. Algebra **304**(2), 679–711 (2006)
21. Kinyon, M.K., Jones, O.: Loops and semidirect products. Comm. Algebra **28**(9), 4137–4164 (2000)
22. Marcus, M., Minc, H.: A Survey of Matrix Theory and Matrix Inequalities. Dover, New York (1992)
23. Nagy, G.P.: Direct construction of code loops. Discrete Math. **308**(23), 5349–5357 (2008)
24. Nagy, G.P., Vojtěchovský, P.: The Moufang loops of order 64 and 81. J. Symbolic Comput. **42**(9), 871–883 (2007)
25. Nagy, P., Strambach, K.: Schreier loops. Czechoslovak Math. J. **58**(133(3)), 759–786 (2008)
26. Pflugfelder, H.O.: Quasigroups and Loops: Introduction. Sigma Series in Pure Mathematics, vol. 7. Heldermann, Berlin (1990)
27. Prószyński, A.: Forms and mappings. I. Generalities. Fund. Math. **122**(3), 219–235 (1984)
28. Prószyński, A.: Forms and mappings. IV. Degree 4. Bull. Polish Acad. Sci. Math. **37**(1–6), 269–278 (1989)
29. Richardson, T.M.: Local subgroups of the Monster and odd code loops. Trans. Amer. Math. Soc. **347**(5), 1453–1531 (1995)
30. Vojtěchovský, P.: Combinatorial polarization, code loops, and codes of high level. Int. J. Math. Math. Sci. **26**, 1533–1541 (2004) (Proceedings of CombinaTexas 2003)
31. Ward, H.N.: Combinatorial polarization. Discrete Math. **26**, 185–197 (1979)