CLASS 2 MOUFANG LOOPS, SMALL FRATTINI MOUFANG LOOPS, AND CODE LOOPS

TIM HSU

Abstract. Let L be a Moufang loop which is centrally nilpotent of class 2. We first show that the nuclearly-derived subloop (normal associator subloop) L^* of L has exponent dividing 6. It follows that L_p (the subloop of L of elements of p-power order) is associative for $p > 3$. Next, a loop L is said to be a *small Frattini Moufang loop*, or SFML, if L has a central subgroup Z of order p such that $C \cong L/Z$ is an elementary abelian p-group. C is thus given the structure of what we call a *coded vector space*, or CVS. (In the associative/group case, CVS's are either orthogonal spaces, for $p = 2$, or symplectic spaces with attached linear forms, for $p > 2$.) Our principal result is that every CVS may be obtained from an SFML in this way, and two SFML's are isomorphic in a manner preserving the central subgroup Z if and only if their CVS's are isomorphic up to scalar multiple. Consequently, we obtain the fact that every SFM 2-loop is a code loop, in the sense of Griess, and we also obtain a relatively explicit characterization of isotopy in SFM 3-loops. (This characterization of isotopy is easily extended to Moufang loops of class 2 and exponent 3.) Finally, we sketch a method for constructing any finite Moufang loop which is centrally nilpotent of class 2.

1. Introduction

The loops (groups without associativity) characterized by the near-associativity property

$$(xy)(zx) = x((yz)x) \tag{1.1}$$

are known as *Moufang loops* (see Pflugfelder [18, Ch. IV]). Many aspects of group theory may be generalized to Moufang loops, and among these aspects is the theory of *central nilpotence* (Bruck [5, Ch. VI]), the loop generalization of nilpotence in groups. Centrally nilpotent Moufang loops have been studied often, and provide many of the basic examples of finite Moufang loops. (See, for instance, Bruck [5, Ch. VIII, Thm. 10.1], Chein [6, II.4], Pflugfelder [18, Ch. IV], and Smith [23, p. 181].) Of particular relevance to this paper is the work of Glauberman and Wright [11, 12],

Date: November 22, 1996.

1991 *Mathematics Subject Classification.* Primary 20N05; Secondary 20D15, 20D08.

Key words and phrases. Centrally nilpotent Moufang loops of class 2, Moufang p-loops, small Frattini Moufang loops, code loops.

who extended many of the standard theorems about finite nilpotent groups to finite centrally nilpotent Moufang loops.

One class of centrally nilpotent Moufang loops which has particularly interesting applications to finite group theory is the class of *code loops.* The first code loop to be recognized as such was the *Parker loop* (named after its discoverer R. A. Parker), which played a key role in Conway's construction of the Monster finite simple group [8]. Subsequently, Griess [13] defined code loops to be certain central extensions of doubly even codes, providing the first published proof of their existence, and then went on [14] to use code loops to construct 2-local subgroups of several other sporadic groups. For more on code loops and finite groups, including further references, see Griess [14] and Richardson [20].

In this paper, we present some new results on centrally nilpotent Moufang loops of class 2, and apply these results by generalizing the theory of extraspecial groups (see, for instance, Aschbacher [1, Ch. 8]) to *small Frattini Moufang loops.* For the convenience of the reader, we now summarize our main results. (The reader who is unfamiliar with the notation and terminology used here may first wish to read Section 2.)

Let L be a Moufang loop which is centrally nilpotent of class 2, that is, a Moufang loop L such that the quotient of L by its center $Z(L)$ is an abelian group; and let L_p be the set of all elements of L whose order is a power of p. Recall that the nuclearly-derived subloop, or normal associator subloop, of L, which we denote by L^*, is the smallest normal subloop of L such that L/L^* is associative (is a group). Recall also that the torsion subloop (subloop of finite order elements) of L is isomorphic to the (restricted) direct product of the subloops L_p, where p runs over all primes (Thm. 6.2 of Bruck [4], our Theorem 3.9, or in the finite case, Cor. 1 of Glauberman and Wright [12]).

In Section 3, we show that the commutator (resp. associator) function is a "symplectic" and "multilinear" function on $L/Z(L) \times L/Z(L)$ (resp. $L/Z(L) \times L/Z(L) \times L/Z(L)$) (Theorem 3.3). As a consequence, we have:

Main Theorem A. *Let L be a Moufang loop which is centrally nilpotent of class 2. Then L^* (as defined above) has exponent dividing 6. In particular, for $p > 3$, L_p (as defined above) is associative (is a group).*

Compare the result of Bruck [5, VIII.2] that the cube of every associator of a commutative Moufang loop is trivial. (In fact, to prove Main Theorem A, we use another case of the same formulas Bruck used to obtain that result.) We also note that Main Theorem A is, in some sense, the best possible result of this type, since Example 3 of VII.5 of Bruck [5] gives a construction of nonassociative finite Moufang p-loops of class 3 for all $p > 2$.

In Sections 4–6, we focus on *small Frattini Moufang loops* (also known as SFM loops, or SFML's), which are Moufang p-loops L with a central subgroup Z of order

p such that $C \cong L/Z$ is an elementary abelian group. (Note that we often think of Z and C as part of the structure of L.) SFML's are a class of Moufang loops often found "in nature." For instance, every extraspecial Moufang loop (Definition 4.1) is an SFML. Also, every code loop is an SFM 2-loop, and conversely:

Main Theorem B. *Every SFM 2-loop is isomorphic to a code loop.*

Compare Thm. 14 of Griess [13], which shows that every loop constructed by "Parker's procedure" (Defn. 13 of Griess [13]) is isomorphic to a code loop. For a more detailed comparison, see Remarks 5.4 and 5.5.

The key to Main Theorem B, and also to Main Theorem C, below, is the fact that L gives C the structure of a *coded vector space*, or *CVS*, over $\mathbf{F}_p$. A CVS is a 4-tuple $(C, \sigma, \chi, \alpha)$, where C is a vector space over $\mathbf{F}_p$, and σ, χ, and α are "symplectic 1-, 2-, and 3-forms" on C which are either multilinear, for $p > 2$, or related by polarization, for $p = 2$.

The relationship between SFML's and CVS's can be stated as follows.

Main Theorem C. *Every CVS can be obtained from some SFML in the manner described above. Furthermore, let L and M be SFML's, with distinguished central subgroups Z_L and Z_M, and associated CVS's C_L and C_M. Then there is an isomorphism $\phi : L \to M$ such that $\phi(Z_L) = Z_M$ if and only if C_L and C_M are isomorphic up to scalar multiple (action of $\mathrm{Aut}(Z_L) = \mathrm{Aut}(Z_M)$).*

The proofs of Main Theorems B and C may be summarized as follows.

Section 4. We define the notion of a *coded extension* of a CVS (Definition 4.9), and show that every SFML is a coded extension of a CVS, and vice versa (Theorem 4.10).

Section 5. We show that every CVS over $\mathbf{F}_2$ can be obtained from a doubly even code (Theorems 5.2 and 5.3). Main Theorem B follows.

Section 6. We show that every CVS has a unique coded extension (Theorems 6.1 and 6.6). Main Theorem C follows.

We remark that the main technical tool used in Section 6, the *semidirect central product*, is also useful for doing calculations in SFML's, especially code loops. In [15], we will address the general topic of decompositions of SFML's as semidirect central products of groups. In particular, we will give some short explicit constructions of code loops, including a Turyn-type construction for the Parker loop. For more details, see Remark 6.7.

Now, as mentioned above, every SFM 3-loop L is a coded extension of some CVS over $\mathbf{F}_3$, say, $(C, \sigma(c), \chi(c,d), \alpha(c,d,e))$. For any $k \in C$, we define the *adjoint translate* $\mathrm{adt}_k(C)$ of C to be the CVS $(C, \sigma(c), \chi(c,d) + \alpha(c,k,d), \alpha(c,d,e))$. A straightforward application of Main Theorem C then gives the following characterization of isotopy in SFM 3-loops (Section 7).

Main Theorem D. *Let L be a coded extension of a CVS $(C, \sigma, \chi, \alpha)$ over $\mathbf{F}_3$. Then up to isomorphism, the loop-isotopes of L are precisely the coded extensions of the adjoint translates of C. In particular, σ and α are "isotopy invariants" of L.*

Furthermore, since Main Theorem C may be generalized directly to Moufang loops of class 2 and exponent 3, Main Theorem D may also be extended to this situation. See Theorem 8.2 for a precise statement.

We conclude in Section 8 by giving a construction which can be used to obtain any finite Moufang loop of class 2. This construction generalizes much previous work, mostly in the commutative case. For instance, compare Bénéteau [2, IV.3], Bruck [3], Chein [6, II.4], and Ray-Chaudhuri and Roth [19].

2. Background and notation

First, we set some conventions and notation to be used throughout.

Notation. Let p be a prime. $\mathbf{F}_p$ denotes the field of order p, and $\mathbf{F}_p^\times$ its nonzero elements. Following group-theoretic custom, unless otherwise specified, we think of $\mathbf{F}_p$ as the group of order p, and $\mathbf{F}_p^\times$ as the automorphism group of $\mathbf{F}_p$. In this context, we identify the vector space $\mathbf{F}_p^k$ with the elementary abelian p-group of rank k, and we write vector addition in $\mathbf{F}_p^k$ multiplicatively, with the zero vector written as 1.

If $a, b, c, \ldots$ are elements or subsets of a loop (resp. vector space), $\langle a, b, c, \ldots \rangle$ denotes the subloop (resp. subspace) generated by $a, b, c, \ldots$.

For those less familiar with loop theory, and for the purpose of establishing notation and terminology, we also review some definitions and results in loop theory, using Pflugfelder [18], Bruck [5], and Chein, Pflugfelder, and Smith [7] as our standard sources.

Definition 2.1. An *inverse property loop*, or in this paper, simply a *loop*, is a set L with a binary operation (written as juxtaposition) having a unique identity element and unique two-sided inverses. (Note that the term "inverse" means that $a^{-1}(ax) = (xa)a^{-1} = x$.) In other words, a loop is a group minus associativity.

Many concepts of group theory may be generalized to loop theory; we highlight the following ones.

Definition 2.2. For loop elements γ, δ, and ϵ, we define the *commutator* $[\gamma, \delta]$ to be $(\delta\gamma)^{-1}(\gamma\delta)$ and the *associator* $[\gamma, \delta, \epsilon]$ to be $(\gamma(\delta\epsilon))^{-1}((\gamma\delta)\epsilon)$. In other words,

$$\gamma\delta = (\delta\gamma)[\gamma, \delta], \tag{2.1}$$

$$(\gamma\delta)\epsilon = (\gamma(\delta\epsilon))[\gamma, \delta, \epsilon], \tag{2.2}$$

$$\gamma(\delta\epsilon) = ((\gamma\delta)\epsilon)[\gamma, \delta, \epsilon]^{-1}. \tag{2.3}$$

(The inexperienced reader should note the inverse in the last formula.)

Definition 2.3. Let L be a loop. The *nucleus* of L (denoted by $N(L)$) is the set of all $z \in L$ such that $[z, x, y] = [x, z, y] = [x, y, z] = 1$ for all $x, y \in L$; and the *center* of L (denoted by $Z(L)$) is defined to be the set of all $z \in N(L)$ such that $[z, x] = 1$ for all $x, y \in L$.

If L is a loop, it can be shown (see Pflugfelder [18, I.3]) that $N(L)$ is a subgroup of L, and that $Z(L)$ is an abelian subgroup of $N(L)$.

Definition 2.4. A *normal* subloop of a loop L is any subloop of L which is the kernel of some homomorphism from L to a loop.

For instance, any *central subgroup* (subgroup of $Z(L)$) of a loop L is normal in L (Pflugfleder [18, I.7]).

Definition 2.5. Let L be a loop. We define the *centrally-derived subloop* (or normal commutator-associator subloop) of L to be the smallest normal subloop $L' \lhd L$ such that L/L' is an abelian group. Similarly, we define the *nuclearly-derived subloop* (or normal associator subloop) of L to be the smallest normal subloop $L^* \lhd L$ such that L/L^* is associative (is a group).

See Bruck [5, Ch. VI] for a proof that L' and L^* are well-defined. Note that it follows from the isomorphism theorems for loops (see Pflugfelder [18, I.7]) that L' (resp. L^*) is the smallest normal subloop of L containing all $[\gamma, \delta]$ and $[\gamma, \delta, \epsilon]$ (resp. all $[\gamma, \delta, \epsilon]$), where γ, δ, ϵ run over all elements of L.

We will use Bruck's theory of central nilpotence [5, Ch. VI], as described in the following definitions and Theorem 2.8.

Definition 2.6. Let L be a loop. The *upper central series* $\{Z_i\}$ of L is defined by letting $Z_0 = 1$ and letting Z_{i+i} be the unique subloop of L containing Z_i such that $Z_{i+i}/Z_i = Z(L/Z_i)$. We say that L is *centrally nilpotent of class* n, or simply of class n, if there exists n such that $Z_n = L$ and $Z_{n-1} \neq L$.

For instance, L is of class 2 if and only if $L/Z(L)$ is an abelian group and L is not, that is, if and only if $1 < L' \leq Z(L)$.

Definition 2.7. The *Frattini subloop* $\Phi(L)$ of a loop L is defined to be the set of *non-generators* of L, that is, the set of all $x \in L$ such that for any subset S of L, $L = \langle x, S\rangle$ implies $L = \langle S\rangle$.

Theorem 2.8. *Let L be a finite centrally nilpotent loop. Then $\Phi(L) \lhd L$, and $L/\Phi(L)$ is isomorphic to a subgroup of the direct product of groups of prime order.*

Proof. This follows immediately from Thms. 2.1 and 2.2 of Ch. VI of Bruck [5]. $\square$

We are particularly interested in loops of the following type.

Definition 2.9. A loop L is said to be *Moufang* if any, and therefore all (see Pflugfelder [18, Ch. IV]), of the following identities hold for all $\gamma, \delta, \epsilon \in L$:

$$((\delta\gamma)\epsilon)\gamma = \delta(\gamma(\epsilon\gamma)), \tag{2.4}$$

$$((\gamma\delta)\gamma)\epsilon = \gamma(\delta(\gamma\epsilon)), \tag{2.5}$$

$$(\gamma(\delta\epsilon))\gamma = (\gamma\delta)(\epsilon\gamma) = \gamma((\delta\epsilon)\gamma). \tag{2.6}$$

Definition 2.10. The *Moufang center* of a Moufang loop L, denoted by $C(L)$, is defined to be the set of all $z \in L$ such that $[z, x] = 1$ for all $x \in L$.

Let L be a Moufang loop. Clearly, $Z(L) = N(L) \cap C(L)$. Furthermore, it can also be shown (see Pflugfelder [18, Thm. IV.3.10]) that $C(L)$ is a subloop of L.

Moufang loops have many near-associativity properties, such as the following consequence of *Moufang's theorem* (see Pflugfelder [18, Ch. IV]).

Theorem 2.11. *Let L be a Moufang loop. Then L is di-associative; that is, for $x, y \in L$, $\langle x, y\rangle$ is associative. In particular, L is power-associative; that is, x^n is well-defined.* □

We will also use the Lagrangian property of di-associative loops (Bruck [5, Thm. V.1.2]), stated as:

Theorem 2.12. *Let L be a finite di-associative (e.g., Moufang) loop. Then the order of any element of L divides the order of L.* □

Definition 2.13. Let L be a power-associative loop, and let p be a prime. We say that L is a *p-loop* if every element of L has order a power of p.

Let L be a di-associative loop. Because of Theorem 2.12, if L has order a power of p, then L is a finite p-loop. Conversely, if L is a finite centrally nilpotent p-loop, the isomorphism theorems for loops imply that the order of L is a power of p. Therefore, since most of the loops we consider are finite centrally nilpotent Moufang loops, we will usually treat the concepts of having order a power of p and being a finite p-loop as interchangable. (In fact, all finite Moufang p-loops are centrally nilpotent; see Glauberman [11, Thm. 4] and Glauberman and Wright [12].)

Finally, we define one last important concept of loop theory.

Definition 2.14. A triple (U, V, W) of bijections from a loop L to a loop M (whose operation is denoted by $\circ$) is called an *isotopism* if, for all $x, y \in L$, $(xU) \circ (yV) = (xy)W$. If an isotopism exists from L to M, we say that M is an *isotope* of L, or that L and M are *isotopic*.

It is worth noting that isotopy plays no role in group theory because every loop-isotope of a group G is isomorphic to G (see Pflugfelder [18, Cor. III.2.3]). More generally, any loop which is isomorphic to all of its loop-isotopes is called a *G-loop*. See Pflugfelder [18, Ch. III] for more on isotopy.

3. Moufang loops of class 2

We first quote the following result, due to Bruck.

Proposition 3.1. *Let L be a Moufang loop such that $[[\gamma,\delta,\epsilon],\gamma]=1$ for all $\gamma,\delta,\epsilon\in L$. Then for all $\gamma,\delta,\epsilon\in L$, $[\gamma,\delta,\epsilon]$ is central in $\langle\gamma,\delta,\epsilon\rangle$, and the following identities hold for all $n\in\mathbf{Z}$:*

$$[\gamma,\delta,\epsilon]=[\delta,\epsilon,\gamma]=[\delta,\gamma,\epsilon]^{-1} \tag{3.1}$$

$$[\gamma^n,\delta,\epsilon]=[\gamma,\delta,\epsilon]^n \tag{3.2}$$

$$[\gamma\delta,\epsilon]=[\gamma,\epsilon][[\gamma,\epsilon],\delta][\delta,\epsilon][\gamma,\delta,\epsilon]^3 \tag{3.3}$$

Note that part of the statement of (3.3) is that the right hand side gives the same result, no matter how the terms are associated.

Proof. This follows from Lemma VII.5.5 of Bruck [5]. □

For the rest of this section, let L be a Moufang loop with a fixed central subgroup Z such that $C\cong L/Z$ is an abelian group. Clearly, such a loop is centrally nilpotent of class 2, and conversely, for any Moufang loop L of class 2, we may take $Z=Z(L)$. By convention, the letters γ, δ, ϵ, and φ refer to elements of L, and their images in the quotient C are denoted by c, d, e, and f, respectively.

Definition 3.2. We define functions $\chi: C\times C\to Z$ and $\alpha: C\times C\times C\to Z$ by the following formulas.

$$\chi(c,d)=[\gamma,\delta], \tag{3.4}$$

$$\alpha(c,d,e)=[\gamma,\delta,\epsilon]. \tag{3.5}$$

Note that χ and α are well-defined because for any $z\in Z$, $[\gamma z,\delta,\epsilon]=[\gamma,\delta,\epsilon]$, and so on.

The following key theorem says that the functions χ and α are "symplectic" ((3.6) and (3.10)), "skew-symmetric" ((3.7) and (3.11)), "power-multilinear" ((3.8) and (3.12)), and related by "polarization" (3.9); and that α is multilinear (3.13).

Theorem 3.3. *For all $c,d,e,f\in C$ and all $n\in\mathbf{Z}$, we have:*

$$\chi(c,c)=1, \tag{3.6}$$

$$\chi(c,d)=\chi(d,c)^{-1}, \tag{3.7}$$

$$\chi(c^n,d)=\chi(c,d)^n, \tag{3.8}$$

$$\chi(cd,e)=\chi(c,e)\chi(d,e)\alpha(c,d,e)^3, \tag{3.9}$$

and

$$\alpha(c,d,d) = \alpha(d,c,d) = \alpha(d,d,c) = 1, \tag{3.10}$$

$$\alpha(c,d,e) = \alpha(d,c,e)^{-1} = \alpha(d,e,c), \tag{3.11}$$

$$\alpha(c^n,d,e) = \alpha(c,d,e)^n, \tag{3.12}$$

$$\alpha(cd,e,f) = \alpha(c,e,f)\alpha(d,e,f). \tag{3.13}$$

Proof. We first note that (3.6) and (3.7) are easy, (3.9) follows from (3.3) and the fact that L' is central, (3.10) follows from di-associativity, (3.11) follows from (3.1), and (3.12) follows from (3.2). Furthermore, (3.9), (3.10), and (3.12) imply

$$\begin{aligned} \chi(c^{n+1},d) &= \chi(c^n,d)\chi(c,d)\alpha(c^n,c,d)^3 \\ &= \chi(c^n,d)\chi(c,d), \end{aligned} \tag{3.14}$$

so (3.8) follows by induction on positive and negative n.

It remains to prove (3.13). Now, by definition,

$$\alpha(cd,e,f) = ((\gamma\delta)(\epsilon\varphi))^{-1}(((\gamma\delta)\epsilon)\varphi), \tag{3.15}$$

and

$$\begin{aligned} ((\gamma\delta)\epsilon)\varphi &= (\gamma(\delta\epsilon))\varphi \cdot \alpha(c,d,e) \\ &= \gamma((\delta\epsilon)\varphi) \cdot \alpha(c,d,e)\alpha(c,de,f) \\ &= \gamma(\delta(\epsilon\varphi)) \cdot \alpha(c,d,e)\alpha(c,de,f)\alpha(d,e,f) \\ &= (\gamma\delta)(\epsilon\varphi) \cdot \alpha(c,d,e)\alpha(c,de,f)\alpha(d,e,f)\alpha(c,d,ef)^{-1}, \end{aligned} \tag{3.16}$$

which means that

$$\alpha(cd,e,f) = \alpha(c,d,e)\alpha(c,de,f)\alpha(d,e,f)\alpha(c,d,ef)^{-1}. \tag{3.17}$$

We claim that (3.13) is a consequence of (3.17).

To prove this claim, by substituting first $c = w$, $d = x$, $e = y$, and $f = z$, and then $c = x$, $d = y$, $e = z$, and $f = w$, into (3.17), we get

$$\alpha(wx,y,z) = \alpha(w,x,y)\alpha(w,xy,z)\alpha(x,y,z)\alpha(w,x,yz)^{-1}, \tag{3.18}$$

$$\alpha(xy,z,w) = \alpha(x,y,z)\alpha(x,yz,w)\alpha(y,z,w)\alpha(x,y,zw)^{-1}. \tag{3.19}$$

Since skew-symmetry implies $\alpha(w,xy,z) = \alpha(xy,z,w)$, we may substitute the right-hand side of (3.19) for the second term in the right-hand side of (3.18). Applying skew-symmetry to collect terms, we obtain

$$\alpha(wx,y,z) = \alpha(wz,y,x)\alpha(w,x,y)\alpha(w,y,z)\alpha(x,y,z)^2. \tag{3.20}$$

We call (3.20) the *exchange identity*, since it implies that we may exchange the x and the z in $\alpha(wx,y,z)$ at the cost of adding the other terms on the right-hand side of (3.20).

Using the exchange identity and skew-symmetry, we see that

$$\begin{aligned}\alpha(c,de,f) &= \alpha(de,f,c)\\ &= \alpha(dc,f,e)\alpha(d,e,f)\alpha(d,f,c)\alpha(e,f,c)^2\\ &= \alpha(cd,e,f)^{-1}\alpha(d,e,f)\alpha(c,d,f)\alpha(c,e,f)^2.\end{aligned}\tag{3.21}$$

Applying exchange and skew-symmetry again, we have

$$\begin{aligned}\alpha(c,d,ef)^{-1} &= \alpha(ef,d,c)\\ &= \alpha(ec,d,f)\alpha(e,f,d)\alpha(e,d,c)\alpha(f,d,c)^2\\ &= \alpha(ce,f,d)^{-1}\alpha(d,e,f)\alpha(c,d,e)^{-1}\alpha(c,d,f)^{-2},\end{aligned}\tag{3.22}$$

and applying exchange and skew-symmetry to the first term of the last expression in (3.22), we have

$$\begin{aligned}\alpha(c,d,ef)^{-1} &= \alpha(cd,f,e)^{-1}\alpha(c,e,f)^{-1}\alpha(c,f,d)^{-1}\alpha(e,f,d)^{-2}\\ &\qquad\cdot\alpha(d,e,f)\alpha(c,d,e)^{-1}\alpha(c,d,f)^{-2},\\ &= \alpha(cd,e,f)\alpha(c,d,e)^{-1}\alpha(c,d,f)^{-1}\alpha(c,e,f)^{-1}\alpha(d,e,f)^{-1}.\end{aligned}\tag{3.23}$$

Finally, substituting (3.21) and (3.23) into (3.17), we get

$$\begin{aligned}\alpha(cd,e,f) &= \alpha(c,d,e)\\ &\qquad\cdot\alpha(cd,e,f)^{-1}\alpha(d,e,f)\alpha(c,d,f)\alpha(c,e,f)^2\\ &\qquad\cdot\alpha(d,e,f)\\ &\qquad\cdot\alpha(cd,e,f)\alpha(c,d,e)^{-1}\alpha(c,d,f)^{-1}\alpha(c,e,f)^{-1}\alpha(d,e,f)^{-1}\\ &= \alpha(c,e,f)\alpha(d,e,f),\end{aligned}\tag{3.24}$$

and the theorem follows. ☐

Remark 3.4. Note that (3.13), which is really the only new formula in Theorem 3.3, has been previously obtained in several special cases, such as the commutative case (Smith [22]) and the code loop case (Griess [13, Lem. 15]).

Remark 3.5. It may be instructive to consider the following method of proving Theorem 3.3 without relying on Bruck's formulas (Proposition 3.1). (In fact, this is how the author first discovered Theorem 3.3.) Now, given the skew-symmetry of α (eq. (3.11)), we can obtain (3.13) as above, and we can obtain (3.9) by calculating the χ and α terms needed to change $(\gamma\delta)\epsilon$ to $\epsilon(\gamma\delta)$, as we did in (3.16). Furthermore, (3.8) and (3.12) follow from (3.9) and (3.13) and di-associativity. Therefore, the crux of the proof lies in obtaining (3.11). In fact, it is here that the Moufang property seems to be used most strongly, as the only proofs of skew-symmetry of which the author is aware rely on the fact that every inner mapping of a Moufang loop is a semi-endomorphism. (This approach involves imitating one part of the proof of Moufang's theorem; see, for example, Pflugfelder [18, IV.2.3].)

Remark 3.6. Schneps (personal communication) has observed that (3.17) is yet another version of the "pentagonal" relation from monoidal categories, and that (3.9) is a version of the "hexagonal" relation from symmetric monoidal categories. See MacLane [17, Ch. VII] for more on these relations; see also Remark 6.8.

In the rest of this section, we describe some of the consequences of Theorem 3.3.

Theorem 3.7. *For $c, d, e \in C$ such that $c^k = d^m = e^n = 1$, the order of $\chi(c, d)$ divides $\gcd(k, m)$, and the order of $\alpha(c, d, e)$ divides $\gcd(k, m, n)$.*

Proof. From (3.8), we have

$$\chi(c, d)^k = \chi(c^k, d) = \chi(1, d) = 1, \tag{3.25}$$

and our commutator claim follows from skew-symmetry. The same proof works for our associator claim. □

For a prime p, define L_p to be the set of all $x \in L$ such that the order of x is a power of p. In the next two theorems (Theorems 3.8 and 3.9) we recover the class 2 case of results of Bruck [4, Thm. 6.2] and Glauberman and Wright [12, Cor. 1].

Theorem 3.8. *L_p is a subloop of L.*

Proof. For $\gamma, \delta \in L_p$, let q be the greater of the orders of γ and δ, and let $r = q(q-1)/2$. Then, using di-associativity and the definition of χ, we have

$$(\gamma\delta)^q = \gamma^q \delta^q \chi(d, c)^r = \chi(d, c)^r, \tag{3.26}$$

and the theorem follows from Theorem 3.7. □

Theorem 3.9. *Let T be the set of all elements of L of finite order. Then T is a subloop of L isomorphic to the restricted direct product of the L_p's, over all primes p.*

Proof. First, we note that Theorem 3.7 implies that elements of relatively prime order commute and associate freely, so the unassociated product of elements of pairwise relatively prime order is well-defined. Consequently, by the Chinese Remainder Theorem, for every $\gamma \in L$ of order n, we have

$$\gamma = \prod_{p|n} \gamma_p, \tag{3.27}$$

where each γ_p is a power of γ, and the order of γ_p is a power of p.

It is therefore enough to show that if the orders of γ_i and δ_j are relatively prime for $i, j = 1, 2$, then $(\gamma_1\delta_1)(\gamma_2\delta_2) = (\gamma_1\gamma_2)(\delta_1\delta_2)$. However, using Theorem 3.7 repeatedly, we see that

$$\begin{aligned}(\gamma_1\delta_1)(\gamma_2\delta_2) &= \gamma_1(\delta_1(\gamma_2\delta_2)) = \gamma_1((\delta_1\gamma_2)\delta_2) = \gamma_1((\gamma_2\delta_1)\delta_2) \\ &= \gamma_1(\gamma_2(\delta_1\delta_2)) = (\gamma_1\gamma_2)(\delta_1\delta_2),\end{aligned} \tag{3.28}$$

and the theorem follows. □

We next obtain Main Theorem A.

Proof of Main Theorem A. Since L^* is an abelian group generated by $\alpha(c,d,e)$ for all $c,d,e \in C$, it is enough to show that $\alpha(c,d,e)^6 = 1$ for all $c,d,e \in C$. However, since (3.9) implies

$$\chi(c,e)\chi(d,e)\alpha(c,d,e)^3 = \chi(cd,e) = \chi(dc,e) = \chi(d,e)\chi(c,e)\alpha(d,c,e)^3, \tag{3.29}$$

using skew-symmetry, we have $\alpha(c,d,e)^3 = \alpha(d,c,e)^3 = \alpha(c,d,e)^{-3}$, and the theorem follows. □

We then have the following analogue of Thm. 11.2 of Bruck [5, Ch. VIII].

Theorem 3.10. *If L is finitely generated, then L^* is finite. More precisely, L is a central extension of L/L^* (a finitely generated group of class ≤ 2) by a finite group of exponent 6.*

Proof. Since (3.13) implies that L^* is an abelian group generated by $\alpha(c,d,e)$, where γ, δ, and ϵ run over all *generators* of L, the theorem follows from Main Theorem A. □

Finally, we note that Moufang loops of class 2 satisfy the following stronger version of the Moufang identity.

Theorem 3.11. *If n is the exponent of L^*, then L satisfies*

$$\gamma^k(\delta(\gamma\epsilon)) = ((\gamma^k\delta)\gamma)\epsilon \tag{3.30}$$

for all $\gamma,\delta,\epsilon \in L$, and precisely those integers k such that $k \equiv 1 \pmod{n}$.

The identity (3.30) is called the *M_k-law.* Note that the M_1-law is just (2.5).

Proof. From the definition of α, we have

$$\begin{aligned} ((\gamma^k\delta)\gamma)\epsilon &= (\gamma^k\delta)(\gamma\epsilon)\alpha(c^kd,c,e) \\ &= \gamma^k(\delta(\gamma\epsilon))\alpha(c^kd,c,e)\alpha(c^k,d,ce). \end{aligned} \tag{3.31}$$

However, using (3.10)–(3.13), we obtain

$$\begin{aligned} \alpha(c^kd,c,e)\alpha(c^k,d,ce) &= \alpha(c^k,c,e)\alpha(d,c,e)\alpha(c^k,d,c)\alpha(c^k,d,e) \\ &= \alpha(c,d,e)^{k-1}, \end{aligned} \tag{3.32}$$

which means that the M_k-law is satisfied if and only if the order of any $\alpha(c,d,e)$ divides $k-1$. The theorem follows. □

We then have the following corollary. (This result on Moufang loops of class 2 can also be obtained more directly from Cor. IV.4.8 of Pflugfelder [18].)

Corollary 3.12. *If $L_3 \cap L^* = 1$, then L is a G-loop.*

Proof. If $L_3 \cap L^* = 1$, then L satisfies an M_k-law for all odd k, and so the corollary follows from Thm. IV.4.11 of Pflugfelder [18]. □

4. Small Frattini Moufang loops and coded vector spaces

In the rest of this paper, we assume all loops are finite; in fact, we will mostly consider loops of prime power order. To motivate our main definition (Definition 4.3), we begin by imitating Sect. 23 of Aschbacher [1].

Definition 4.1. Let p be a prime. We say that a Moufang p-loop L is *special* if $\Phi(L) = Z(L) = L'$, and we say that a special Moufang loop L is *extraspecial* if $Z(L)$ is cyclic.

For instance, every extraspecial group is an extraspecial Moufang loop.

Note that every nontrivial special Moufang loop is centrally nilpotent of class 2. Theorem 2.8 therefore implies that if L is a special Moufang loop, then $L/\Phi(L)$ is an elementary abelian group. Furthermore, copying the proof of (23.7) in Aschbacher [1] word for word, it also follows that $Z(L)$ is an elementary abelian group. We conclude that L is an extraspecial Moufang loop if and only if $\Phi(L) = Z(L) = L'$ has order p.

Remark 4.2. As the reader may have noticed, Main Theorem A implies that Definition 4.1 is new only when $p = 2$ or 3; otherwise, we are talking about (extra)special groups. However, since it requires little extra effort, we will continue to discuss the case of arbitrary p.

We generalize our situation slightly with the following definition.

Definition 4.3. A p-loop L is said to be *small Frattini* if $\Phi(L)$ has order dividing p. A small Frattini loop L is said to be *central small Frattini* if $\Phi(L) \leq Z(L)$.

For instance, every extraspecial Moufang loop is central small Frattini, as is any elementary abelian group. More generally:

Theorem 4.4. *Every small Frattini Moufang loop is central small Frattini.*

Recall that $C(L)$ denotes the Moufang center of a Moufang loop L (Definition 2.10).

Proof. Let L be a small Frattini Moufang loop. The theorem is clear for groups, so since $L^* \leq L' \leq \Phi(L)$, we may assume that $L^* = \Phi(L)$ has order p. It follows that for some $\gamma, \delta, \epsilon \in L$, $A = [\gamma, \delta, \epsilon] \neq 1$ and $L^* = \langle A \rangle$. Now, for all $y \in L$, $\langle A \rangle$ is a normal subgroup of order p in $\langle A, y \rangle$, so $[A, y] = 1$. In other words, $L^* = \langle A \rangle \leq C(L)$.

Therefore, it is enough to show that $A \in N(L)$. Furthermore, since we now know that Proposition 3.1 applies to L, it is enough to show that $a = [A, \delta, \epsilon] = 1$ for any $\delta, \epsilon \in L$. However, for any $\delta, \epsilon \in L$, Proposition 3.1 implies that $a = [A, \delta, \epsilon]$ is central in $\langle A, \delta, \epsilon \rangle$, so if $a \neq 1$, then $\langle A \rangle = L^* = \langle a \rangle = Z(\langle \gamma, \delta, \epsilon \rangle)$, a contradiction. The theorem follows. ∎

Notation. In the rest of this paper, we abbreviate the term "small Frattini Moufang" as SFM, and we abbreviate "small Frattini Moufang loop" as SFML. Also, for the rest of this section, let p be a prime, let L be an SFML of order p^{1+k}, let Z be a fixed central subgroup of L, and let $C \cong L/Z$ be an elementary abelian p-group of rank k (vector space of dimension k over $\mathbf{F}_p$). We also retain the convention of the previous section that $\gamma, \delta, \epsilon, \varphi \in L$ reduce to $c, d, e, f \in C$ in the quotient.

Applying Theorem 3.3, we see that χ and α are again well-defined functions which satisfy the formulas (3.6)–(3.13). However, to understand SFML's, we need one more function.

Definition 4.5. We define the function $\sigma : C \to Z$ by $\sigma(c) = \gamma^p$. Note that σ is well-defined because Z is central and has exponent p and L/Z has exponent p.

The following is the analogue of Theorem 3.3 for σ.

Theorem 4.6. *For all $c, d \in C$, we have:*

$$\sigma(c^n) = \sigma(c)^n \tag{4.1}$$

$$\sigma(cd) = \begin{cases} \sigma(c)\sigma(d)\chi(c,d) & \text{for } p = 2, \\ \sigma(c)\sigma(d) & \text{for } p > 2. \end{cases} \tag{4.2}$$

Proof. (4.1) is clear. As for (4.2), if $r = p(p-1)/2$, then

$$(\gamma\delta)^p = \gamma^p\delta^p\chi(d,c)^r = \sigma(c)\sigma(d)\chi(d,c)^r. \tag{4.3}$$

The theorem follows from the fact that for $p > 2$, p divides r, and for $p = 2$, $r = 1$ and $\chi(c,d) = \chi(d,c)$. □

We are led to the following definition.

Definition 4.7. Let Z be the group of order p. A *coded vector space* (or CVS) is defined to be a 4-tuple $(C, \sigma, \chi, \alpha)$, where C is a finite-dimensional vector space over $\mathbf{F}_p$, and $\sigma : C \to Z$, $\chi : C \times C \to Z$, and $\alpha : C \times C \times C \to Z$ satisfy (4.1)–(4.2), (3.6)–(3.9), and (3.10)–(3.13), for all $c, d, e, f \in C$ and all $n \in \mathbf{Z}$.

Notation. We will often refer to the CVS $(C, \sigma, \chi, \alpha)$ simply as C.

It is worth noting the different forms that (4.2) and (3.9) take for different p. That is, for $p = 2$, we have

$$\sigma(cd) = \sigma(c)\sigma(d)\chi(c,d), \tag{4.4}$$

$$\chi(cd,e) = \chi(c,e)\chi(d,e)\alpha(c,d,e), \tag{4.5}$$

and for $p > 2$, we have

$$\sigma(cd) = \sigma(c)\sigma(d), \tag{4.6}$$

$$\chi(cd,e) = \chi(c,e)\chi(d,e). \tag{4.7}$$

In other words, for $p = 2$, σ, χ, and α are related by polarization, and for $p > 2$, σ and χ are multilinear. As for α, for $p = 2$ or 3, α is multilinear, and for $p > 3$, α is identically equal to 1.

We also note that (4.1), (3.8), and (3.12) imply

$$\sigma(1) = \chi(c, 1) = \alpha(c, d, 1) = 1 \tag{4.8}$$

for all $c, d \in C$.

Note that choosing a different generator for Z has the effect of acting on σ, χ, and α by an element of $\mathrm{Aut}(Z)$; in additive terms, this means that C is really only defined up to scalar multiple. The natural definition of isomorphism for CVS's is therefore the following one.

Definition 4.8. Let $(C_i, \sigma_i, \chi_i, \alpha_i)$ be a CVS for $i = 1, 2$. We say that C_1 and C_2 are *isomorphic up to scalar multiple* if there is a vector space isomorphism $\phi : C_1 \to C_2$ and some fixed $a \in \mathrm{Aut}(Z)$ such that

$$\begin{aligned} \sigma_2(\phi(c)) &= \sigma_1(c)^a, \\ \chi_2(\phi(c), \phi(d)) &= \chi_1(c, d)^a, \\ \alpha_2(\phi(c), \phi(d), \phi(e)) &= \alpha_1(c, d, e)^a. \end{aligned} \tag{4.9}$$

If C_1 and C_2 are isomorphic up to scalar multiple with respect to the trivial scalar (identity automorphism of Z), then we say that C_1 and C_2 are *isomorphic.*

Finally, to describe the relationship between SFML's and CVS's, we introduce one more definition, in which, by convention, we define γ^n inductively by $\gamma^0 = 1$ and $\gamma^{n+1} = \gamma\gamma^n$.

Definition 4.9. Let p be a prime, and let $(C, \sigma, \chi, \alpha)$ be a CVS over $\mathbf{F}_p$. We say that a loop L is a *coded extension* of C if L satisfies the following conditions.

1. L has a central subgroup Z of order p such that $L/Z \cong C$.
2. Let $\gamma, \delta, \epsilon \in L$ denote arbitrary preimages of $c, d, e \in C$, respectively. Then:

$$\gamma^p = \sigma(c), \tag{4.10}$$

$$[\gamma, \delta] = \chi(c, d), \tag{4.11}$$

$$[\gamma, \delta, \epsilon] = \alpha(c, d, e), \tag{4.12}$$

where the values of σ, χ, and α are taken to be in the central subgroup Z.

Theorem 4.10. *Every SFML is a coded extension of a CVS, and every coded extension of a CVS is an SFML.*

Proof. If L is a Moufang loop with a central subgroup Z of order p such that $C \cong L/Z$ is an elementary abelian p-group, Theorems 3.3 and 4.6 imply that L is a coded extension of the CVS $(C, \sigma, \chi, \alpha)$, where σ, χ, and α are from Definitions 3.2 and 4.5. Conversely, let L be a coded extension of a CVS $(C, \sigma, \chi, \alpha)$. Because α satisfies (3.10)–(3.13), the proof of Theorem 3.11 in the case $k = 1$ shows that L is Moufang. (Note that for $k = 1$, the proof of Theorem 3.11 does not use power-associativity.) Therefore, since L/Z is an elementary abelian p-group, L is an SFML. $\square$

5. Coded vector spaces and doubly even codes

We come to the question: Given an m-dimensional vector space C over $\mathbf{F}_p$, in what ways can σ, χ, and α be defined to obtain a CVS? Now, for $p > 2$, (4.6) and (4.7) show that σ, χ, and α can be chosen independently, which makes this question easy. On the other hand, for $p = 2$, σ, χ, and α are related by polarization, so it is less clear *a priori* which CVS's exist over $\mathbf{F}_2$.

Let C be a CVS over $\mathbf{F}_2$, and let $\{c_1 \dots c_m\}$ be a basis for C. Clearly, the symplectic, skew-symmetric (or in characteristic 2, symmetric), and polarization properties of σ, χ, and α imply that σ, χ, and α are determined by $\sigma(c_i)$ $(1 \leq i \leq m)$, $\chi(c_i, c_j)$ $(1 \leq i < j \leq m)$, and $\alpha(c_i, c_j, c_k)$ $(1 \leq i < j < k \leq m)$. Conversely, as we shall see in a moment, we may define a valid σ, χ, and α by setting these values arbitrarily. Now, it is possible to prove this directly (see Theorem 8.3), but we will instead show that every CVS over $\mathbf{F}_2$ can be obtained from a *doubly even code* (Theorem 5.3).

Notation. For the rest of this section, we revert to additive notation for $\mathbf{F}_2$.

Definition 5.1. A *binary code* (or in this paper, simply a code) of length n and dimension m is defined to be a subspace of $\mathbf{F}_2^n$ of dimension m. We define $|c|$ (resp. $|c \cap d|$, $|c \cap d \cap e|$) to be the number of non-0 coordinates in c (resp. common to c and d, common to c, d, and e). We say that a code C is *doubly even* if $|c| \equiv 0 \pmod 4$ for all $c \in C$.

Note that if C is doubly even, then $|c \cap d| \equiv 0 \pmod 2$ for all $c, d \in C$. Conversely, if $\{c_i\}$ is a basis for a code C, it is easy to see that C is doubly even if and only if $|c_i| \equiv 0 \pmod 4$ and $|c_i \cap c_j| \equiv 0 \pmod 2$ for all c_i and c_j in the basis.

Doubly even codes determine CVS's in the following manner.

Theorem 5.2. *Let C be a doubly even code, and define*

$$\sigma(c) \equiv \frac{|c|}{4} \pmod 2, \tag{5.1}$$

$$\chi(c, d) \equiv \frac{|c \cap d|}{2} \pmod 2, \tag{5.2}$$

$$\alpha(c, d, e) \equiv |c \cap d \cap e| \pmod 2, \tag{5.3}$$

for all $c, d, e \in C$. Then $(C, \sigma, \chi, \alpha)$ is a CVS.

Proof. The symmetry of χ and α is clear, as are (4.1), (3.8), and (3.12). Furthermore, χ, resp. α, is symplectic ((3.6), resp. (3.10)) because $|c| \equiv 0 \pmod 4$, resp. $|c \cap d| \equiv 0 \pmod 2$, for all $c, d \in C$. As for polarization ((4.4), (4.5), and (3.13)), suppose we associate with each $c \in C$ a diagonal matrix M_c with integer entries of 0's and 1's corresponding to the coordinates of c. Then $|c| = \operatorname{trace} M_c$, $|c \cap d| = \operatorname{trace}(M_c M_d)$, and $|c \cap d \cap e| = \operatorname{trace}(M_c M_d M_e)$, which means that

$$M_{cd} = M_c + M_d - 2M_cM_d \tag{5.4}$$

implies polarization. □

Conversely, we have:

Theorem 5.3. *For any integer $m > 0$, choose elements σ_i $(1 \leq i \leq m)$, χ_{ij} $(1 \leq i < j \leq m)$, and α_{ijk} $(1 \leq i < j < k \leq m)$ of $\mathbf{F}_2$. There exists a (unique) CVS $C = \langle c_1 \dots c_m \rangle$ of dimension m such that $\sigma(c_i) = \sigma_i$ $(1 \leq i \leq m)$, $\chi(c_i, c_j) = \chi_{ij}$ $(1 \leq i < j \leq m)$, and $\alpha(c_i, c_j, c_k) = \alpha_{ijk}$ $(1 \leq i < j < k \leq m)$. Furthermore, C is isomorphic (as a CVS) to a doubly even code.*

Proof. Proceeding by induction on m, it suffices to construct a code C which has the required values of σ, χ, and α on its basis. For $m = 1$, if $\sigma_1 = 0$, we may take $C = \langle (1,1,1,1,1,1,1,1) \rangle$, and if $\sigma_1 = 1$, we may take $C = \langle (1,1,1,1) \rangle$. By induction, then, let $C_0 = \langle c_1 \dots c_{m-1} \rangle$ be a doubly even code with the correct values of σ, χ, and α on all basis vectors with indices $< m$. We construct C using the following steps.

1. If $\sigma_m = 0$ (resp. $\sigma_m = 1$), extend C_0 by 8 (resp. 4) coordinates, extend the basis vectors $c_1 \dots c_{m-1}$ by 0's, and add a new vector c_m with all coordinates 0 except the last 8 (resp. 4). The resulting doubly even code C_1 then has the correct values of σ on the basis, and the correct values for χ and α on the basis when all of the indices are $< m$; however, $\chi(c_i, c_m) = 0$ for $1 \leq i < m$ and $\alpha(c_i, c_j, c_m) = 0$ for $1 \leq i < j < m$.
2. For each $i < m$ such that $\chi_{im} = 1$, extend C_1 by 14 coordinates, extend c_i and c_m by

$$\begin{array}{c|cccccccccccccc} c_i & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ c_m & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1, \end{array} \tag{5.5}$$

   and extend the other basis vectors by 0's. The resulting code C_2 has the correct values of σ and χ on the basis, so it remains to correct α.
3. For each $i < j < m$ such that $\alpha_{ijm} = 1$, extend C_2 by 13 coordinates, extend c_i, c_j, and c_m by

$$\begin{array}{c|ccccccccccccc} c_i & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 0 & 0 \\ c_j & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 1 & 0 \\ c_m & 1 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 1 & 0 & 0 & 1, \end{array} \tag{5.6}$$

   and extend the other basis vectors by 0's. The resulting code C has the correct values of σ, χ, and α on the basis, and the theorem follows. □

Main Theorem B now follows.

Proof of Main Theorem B. If C is a doubly even code, it is easy to see that the coded extensions of C are precisely the code loops over C. (Compare Conway [8] and Griess [13].) Therefore, Main Theorem B follows from Theorems 4.10, 5.2, and 5.3. □

Remark 5.4. Griess (personal communication) has suggested the following alternate proof for Main Theorem B. Now, it is not hard to see that the function σ of a CVS over $\mathbf{F}_2$ is a Parker function, as described in Defn. 13 of Griess [13]. (For instance, use (8.7), below.) This fact and Theorem 4.10 imply that every SFM 2-loop is a loop constructed by "Parker's procedure", which means that Main Theorem B follows from Thm. 14 of Griess [13]. In other words, in this approach, Griess' Thm. 14 replaces Theorems 5.2 and 5.3.

Remark 5.5. Note that there are many ways of expressing a given SFM 2-loop as a code loop. For instance, let $\{c, d, e\}$ be a basis for the CVS of the octonion loop (the standard double basis for the octonions). Then, in additive notation,

$$\sigma(c) = \sigma(d) = \sigma(e) = \chi(c, d) = \chi(c, e) = \chi(d, e) = \alpha(c, d, e) = 1. \tag{5.7}$$

Therefore, applying the procedure in the proof of Theorem 5.3, we obtain a doubly even code of length $3(4) + 3(14) + 13 = 67$, the code loop of which is the octonions. On the other hand, applying the procedure in Thm. 14 of Griess [13] to the Parker loop structure of the octonions gives a code of length 38. It is also easily shown that the octonions are the code loop over the Hamming $[7, 3, 4]$ code.

6. Existence and uniqueness of coded extensions

Because of Theorem 4.10, to obtain Main Theorem C, it remains to show that every CVS has a unique coded extension, which we do in this section (Theorems 6.1 and 6.6). Now, for code loops ($p = 2$), this is Thm. 10 of Griess [13], and for $p > 3$, we are in the associative case, which means that this is essentially known. However, to gain insight into the known cases and to introduce the *semidirect central product* (Definition 6.2), we continue to consider all primes p.

Notation. In this section, we use script letters $\mathcal{C}, \mathcal{D}, \mathcal{E}, \dots$ to denote coded extensions of the CVS's $C, D, E, \dots$, possibly with subscripts.

We first address uniqueness. Our proof follows §2 of Conway [8].

Theorem 6.1. *For $n = 1, 2$, let C_n be a CVS of dimension k over $\mathbf{F}_p$, and let $\mathcal{C}_n$ be a coded extension of C_n. If C_1 and C_2 are isomorphic up to scalar multiple, then $\mathcal{C}_1$ is isomorphic to $\mathcal{C}_2$.*

Proof. First, by choosing a different generator for the distinguished central subgroup of $\mathcal{C}_2$, we may assume that C_1 and C_2 are isomorphic. So let $\{c_i\}$ be a basis for

$(C, \sigma, \chi, \alpha) = C_1$, and let $\mathcal{C}$ be the loop given by the loop presentation

$$\langle\, z, \gamma_i \;|$$

$$\gamma_i^p = \sigma(c_i), \tag{6.1}$$

$$[\gamma, \delta] = \chi(c, d), \tag{6.2}$$

$$[\gamma, \delta, \epsilon] = \alpha(c, d, e), \tag{6.3}$$

$$z^p = 1 \,\rangle, \tag{6.4}$$

where i runs between 1 and k; γ, δ, ϵ run over all loop words in the generators; c, d, e are the images in C of γ, δ, ϵ, respectively, under the map sending γ_i to c_i and z to 1; the values of σ, χ, and α are taken to be in $Z = \langle z \rangle$, which is a central subgroup of $\mathcal{C}$ because of (6.2)–(6.4) and (4.8); and the expression γ_i^p is defined inductively by $\gamma_i^0 = 1$ and $\gamma_i^{n+1} = \gamma_i \gamma_i^n$.

Now, since isomorphisms take bases to bases, the above presentation is purely a function of the isomorphism class of C. Therefore, it is enough to show that any coded extension of C is isomorphic to $\mathcal{C}$. Furthermore, since the universal property of loop presentations (see Evans [10, I.2]) implies that *any* coded extension of C is a homomorphic image of $\mathcal{C}$, it is enough to show that $\mathcal{C}$ has order at most p^{1+k}. However, since (6.2)–(6.4) imply that Z is a central subgroup of $\mathcal{C}$ of order dividing p, and (6.1)–(6.3) implies that $\mathcal{C}/Z$ is an elementary abelian p-group of rank k, the theorem follows. $\square$

Notation. We resume the convention that if γ, δ, ϵ (possibly with subscripts) are elements of a coded extension, then c, d, e (possibly with subscripts) are the corresponding elements of the quotient CVS.

We turn to existence. Now, if $\mathcal{D}$ and $\mathcal{E}$ are subloops of the same coded extension, then for $\delta_i \in \mathcal{D}$, $\epsilon_i \in \mathcal{E}$, $(\delta_1\epsilon_1)(\delta_2\epsilon_2) = z_0(\delta_1\delta_2)(\epsilon_1\epsilon_2)$, where $z_0 \in Z$ is expressible in terms of χ, α, d_1, e_1, d_2 and e_2. This observation motivates the following defintion.

Definition 6.2. Let p be a prime and let $Z = \mathbf{F}_p$ be the group of order p. Let D and E be linearly independent subspaces of a CVS $(C, \sigma, \chi, \alpha)$; note that D and E are CVS's by restriction. Let $\mathcal{D}$ (resp. $\mathcal{E}$) be a coded extension of D (resp. E). It is easily verified that the binary operation on the set $Z \times \mathcal{D} \times \mathcal{E}$ given by

$$(z_1, \delta_1, \epsilon_1)(z_2, \delta_2, \epsilon_2) = (z_0 z_1 z_2, \delta_1\delta_2, \epsilon_1\epsilon_2), \tag{6.5}$$

where

$$z_0 = \chi(e_1, d_2)\alpha(d_1, e_1 d_2^{-1}, e_2)\alpha(d_1, e_1, d_2)^2\alpha(e_1, d_2, e_2)^{-2}, \tag{6.6}$$

defines a loop Γ containing the central subgroup $Z \times Z \times Z$. We may therefore define the *semidirect central product* of $\mathcal{D}$ and $\mathcal{E}$ to be the quotient of Γ by the central subgroup $\langle (z, z^{-1}, 1), (z, 1, z^{-1}) \rangle$, where z runs over all elements of Z.

Note that for $p = 2$, (6.6) becomes

$$z_0 = \chi(e_1, d_2)\alpha(d_1, e_1 d_2, e_2), \tag{6.7}$$

for $p = 3$, (6.6) becomes

$$z_0 = \chi(e_1, d_2)\alpha(d_1, e_1 d_2^{-1}, e_2)\alpha(d_1, e_1, d_2)^{-1}\alpha(e_1, d_2, e_2), \tag{6.8}$$

and for $p > 3$,

$$z_0 = \chi(e_1, d_2). \tag{6.9}$$

Notation. Imitating the ATLAS [9] notation $\mathcal{D} \bigcirc \mathcal{E}$ for the central product of two groups $\mathcal{D}$ and $\mathcal{E}$, we use $\mathcal{D} \oplus \mathcal{E}$ to denote the semidirect central product ("central product up to sign") of two code loops $\mathcal{D}$ and $\mathcal{E}$. Note that if the χ and α factors on the right-hand side of (6.5) are always 1, then $\mathcal{D} \oplus \mathcal{E}$ just becomes the ordinary central product. In this situation, we write $\mathcal{D} \bigcirc \mathcal{E}$, just as in the group case.

Theorem 6.3. *Let D and E be linearly independent sub-CVS's of $(C, \sigma, \chi, \alpha)$, let $\mathcal{D}$ (resp. $\mathcal{E}$) be a coded extension of D (resp. E), and let $\mathcal{C} = \mathcal{D} \oplus \mathcal{E}$. Then $\mathcal{C}$ is a coded extension of $D \oplus E$.*

Throughout the following proof, by convention, $\gamma = (z, \delta, \epsilon)$, possibly with subscripts. (Note that by our usual convention, we then have $c = de$.) We also freely identify Z with $Z \times 1 \times 1$. Finally, the "skew-symmetric," "symplectic," and "multilinear" properties of χ and α ((3.6)–(3.13)) will be applied freely.

Proof. First, taking the quotient of $Z \times Z \times Z$ in $\mathcal{C}$ as our distinguished central subgroup, it is easy to see that condition 1 of Definition 4.9 holds in $\mathcal{C}$. Furthermore, by collecting "signs" (elements of Z), it is easy to see that (4.10)–(4.12) hold "up to sign," so it remains to check the signs.

We first verify (4.10), recalling our convention that γ^n is defined inductively by $\gamma^0 = 1$ and $\gamma^{n+1} = \gamma\gamma^n$. First, we claim that for all $n \geq 0$,

$$\gamma^n = (z^n \chi(e, d)^r, \delta^n, \epsilon^n) \tag{6.10}$$

where $r = n(n-1)/2$. In fact, if (6.10) holds, then

$$\begin{aligned} \gamma^{n+1} &= \gamma\gamma^n \\ &= (z, \delta, \epsilon)(z^n \chi(e, d)^r, \delta^n, \epsilon^n) \\ &= (z^{n+1}\chi(e, d)^r \chi(e, d^n), \delta^{n+1}, \epsilon^{n+1}) \\ &= (z^{n+1}\chi(e, d)^{r+n}, \delta^{n+1}, \epsilon^{n+1}), \end{aligned} \tag{6.11}$$

and since $r + n = n(n+1)/2$, (6.10) follows by induction. In particular, if $n = p$, $r = p(p-1)/2$, which means that $\chi(e, d)^r = \chi(d, e)$ for $p = 2$ and $\chi(e, d)^r = 1$ for

$p > 2$. Therefore, collecting signs, we get

$$\begin{aligned}\gamma^p &= (\chi(e,d)^r, \sigma(d), \sigma(e)) \\ &= \begin{cases} \sigma(d)\sigma(e)\chi(d,e) & \text{for } p = 2 \\ \sigma(d)\sigma(e) & \text{for } p > 2 \end{cases} \\ &= \sigma(de) \\ &= \sigma(c).\end{aligned} \tag{6.12}$$

Next, turning to (4.11), by collecting signs, we see that

$$\gamma_1\gamma_2 = (z_3 z_1 z_2, \delta_1\delta_2, \epsilon_1\epsilon_2), \tag{6.13}$$

where

$$z_3 = \chi(e_1, d_2)\alpha(d_1, e_1 d_2^{-1}, e_2)\alpha(d_1, e_1, d_2)^2\alpha(e_1, d_2, e_2)^{-2}; \tag{6.14}$$

and

$$\gamma_2\gamma_1 = (z_4 z_1 z_2, \delta_1\delta_2, \epsilon_1\epsilon_2), \tag{6.15}$$

where

$$\begin{aligned} z_4 = \chi(e_2, d_1)&\chi(d_2, d_1)\chi(e_2, e_1) \\ &\alpha(d_2, e_2 d_1^{-1}, e_1)\alpha(d_2, e_2, d_1)^2\alpha(e_2, d_1, e_1)^{-2}.\end{aligned} \tag{6.16}$$

To obtain (4.11), we need to show that $z = z_3 z_4^{-1} = \chi(d_1 e_1, d_2 e_2)$. However, gathering the χ terms of z, we have

$$\begin{aligned}\chi(e_1, d_2)&\chi(e_2, d_1)^{-1}\chi(d_2, d_1)^{-1}\chi(e_2, e_1)^{-1} \\ &= \chi(e_1, d_2)\chi(d_1, e_2)\chi(d_1, d_2)\chi(e_1, e_2) \\ &= \chi(d_1, d_2 e_2)\chi(e_1, d_2 e_2)\alpha(d_1, d_2, e_2)^3\alpha(e_1, d_2, e_2)^3 \\ &= \chi(d_1 e_1, d_2 e_2)\alpha(d_1, e_1, d_2 e_2)^3\alpha(d_1 e_1, d_2, e_2)^3,\end{aligned} \tag{6.17}$$

and gathering the α terms of z, we have

$$\begin{aligned}&\alpha(d_1, e_1 d_2^{-1}, e_2)\alpha(d_1, e_1, d_2)^2\alpha(e_1, d_2, e_2)^{-2} \\ &\cdot \alpha(d_2, e_2 d_1^{-1}, e_1)^{-1}\alpha(d_2, e_2, d_1)^{-2}\alpha(e_2, d_1, e_1)^2 \\ &= \alpha(d_1, e_1, d_2)^3\alpha(d_1, e_1, e_2)^3\alpha(d_1, d_2, e_2)^3\alpha(e_1, d_2, e_2)^3.\end{aligned} \tag{6.18}$$

(4.11) follows because $\alpha^6 = 1$ identically.

Finally, using the same strategy to verify (4.12), we see that $(\gamma_1\gamma_2)\gamma_3 = z\cdot\gamma_1(\gamma_2\gamma_3)$, where

$$\begin{aligned}
z = {}& \chi(e_1,d_2)\alpha(d_1,e_1d_2^{-1},e_2)\alpha(d_1,e_1,d_2)^2\alpha(e_1,d_2,e_2)^{-2}\\
&\cdot\chi(e_1e_2,d_3)\alpha(d_1d_2,e_1e_2d_3^{-1},e_3)\alpha(d_1d_2,e_1e_2,d_3)^2\alpha(e_1e_2,d_3,e_3)^{-2}\\
&\cdot\chi(e_2,d_3)^{-1}\alpha(d_2,e_2d_3^{-1},e_3)^{-1}\alpha(d_2,e_2,d_3)^{-2}\alpha(e_2,d_3,e_3)^2\\
&\cdot\chi(e_1,d_2d_3)^{-1}\alpha(d_1,e_1d_2^{-1}d_3^{-1},e_2e_3)^{-1}\alpha(d_1,e_1,d_2d_3)^{-2}\alpha(e_1,d_2d_3,e_2e_3)^2\\
&\cdot\alpha(d_1,d_2,d_3)\alpha(e_1,e_2,e_3).
\end{aligned}$$

Collecting the χ terms of z, we have

$$\begin{aligned}
&\chi(e_1,d_2)\chi(e_1e_2,d_3)\chi(e_2,d_3)^{-1}\chi(e_1,d_2d_3)^{-1}\\
&\quad=\chi(e_1,d_2)\chi(e_1,d_3)\chi(e_2,d_3)\alpha(e_1,e_2,d_3)^3\\
&\qquad\chi(e_2,d_3)^{-1}\chi(e_1,d_2)^{-1}\chi(e_1,d_3)^{-1}\alpha(e_1,d_2,d_3)^3\\
&\quad=\alpha(e_1,e_2,d_3)^3\alpha(e_1,d_2,d_3)^3.
\end{aligned}\tag{6.19}$$

Completely expanding all α terms of z and collecting all terms which repeat subscripts, we have

$$\begin{aligned}
&\alpha(d_1,e_1,e_2)\alpha(d_1,d_2^{-1},e_2)\alpha(d_1,e_1,d_2)^2\alpha(e_1,d_2,e_2)^{-2}\\
&\cdot\alpha(d_1,d_3^{-1},e_3)\alpha(d_2,d_3^{-1},e_3)\alpha(d_1,e_1,e_3)\alpha(d_2,e_2,e_3)\\
&\cdot\alpha(d_1,e_1,d_3)^2\alpha(d_2,e_2,d_3)^2\alpha(e_1,d_3,e_3)^{-2}\alpha(e_2,d_3,e_3)^{-2}\\
&\cdot\alpha(d_2,e_2,e_3)^{-1}\alpha(d_2,d_3^{-1},e_3)^{-1}\alpha(d_2,e_2,d_3)^{-2}\alpha(e_2,d_3,e_3)^2\\
&\cdot\alpha(d_1,e_1,e_2)^{-1}\alpha(d_1,e_1,e_3)^{-1}\alpha(d_1,d_2^{-1},e_2)^{-1}\alpha(d_1,d_3^{-1},e_3)^{-1}\\
&\cdot\alpha(d_1,e_1,d_2)^{-2}\alpha(d_1,e_1,d_3)^{-2}\alpha(e_1,d_2,e_2)^2\alpha(e_1,d_3,e_3)^2=1,
\end{aligned}\tag{6.20}$$

since (thankfully) every term in the first three lines of (6.20) is cancelled by some term in the next three lines.

The remaining α terms of z are then, after expansion,

$$\begin{aligned}
&\alpha(d_1,e_2,e_3)\alpha(d_2,e_1,e_3)\alpha(d_1,e_2,d_3)^2\alpha(d_2,e_1,d_3)^2\\
&\cdot\alpha(d_1,d_2^{-1},e_3)^{-1}\alpha(d_1,d_3^{-1},e_2)^{-1}\alpha(e_1,d_2,e_3)^2\alpha(e_1,d_3,e_2)^2\\
&\cdot\alpha(d_1,d_2,d_3)\alpha(e_1,e_2,e_3)\\
&=\alpha(d_1,e_2,e_3)\alpha(e_1,d_2,e_3)^{-1}\alpha(d_1,e_2,d_3)^2\alpha(e_1,d_2,d_3)^{-2}\\
&\cdot\alpha(d_1,d_2,e_3)\alpha(d_1,e_2,d_3)^{-1}\alpha(e_1,d_2,e_3)^2\alpha(e_1,e_2,d_3)^{-2}\\
&\cdot\alpha(d_1,d_2,d_3)\alpha(e_1,e_2,e_3)\\
&=\alpha(d_1,e_2,e_3)\alpha(d_1,e_2,d_3)\alpha(e_1,d_2,d_3)^{-2}\\
&\cdot\alpha(d_1,d_2,e_3)\alpha(e_1,d_2,e_3)\alpha(e_1,e_2,d_3)^{-2}\\
&\cdot\alpha(d_1,d_2,d_3)\alpha(e_1,e_2,e_3).
\end{aligned}\tag{6.21}$$

Multiplying (6.19)–(6.21), we see that $z = \alpha(d_1e_1, d_2e_2, d_3e_3)$, so (4.12), and the theorem, follow. □

Remark 6.4. Compare Kitazume [16], whose Thm. 2 is a particular example of the $p = 2$ case of the above theorem.

With Theorem 6.3, to obtain the existence of coded extensions, we just need the following example.

Example 6.5. Let $(C, \sigma, 1, 1)$ be a CVS of dimension 1, and let c be a nonzero vector in C. If $\sigma(c) = 1$, then $Z \times C$ is a coded extension of C; otherwise, the cyclic group of order p^2 is a coded extension of C.

Theorem 6.6. *If C is a CVS, there is a (unique) coded extension of C.*

Proof. Proceeding by induction on $k = \dim C$, let $C = D + E$, where $\dim D = k - 1$ and $\dim E = 1$, let $\mathcal{D}$ be the coded extension of D (by induction), and let $\mathcal{E}$ be the coded extension of E (from Example 6.5). Then from Theorem 6.3, $\mathcal{D} \oplus \mathcal{E}$ is a coded extension of C. □

Remark 6.7. Consider again the loop $\mathcal{C}$ given by the presentation in the proof of Theorem 6.1. Now, there is an easy "solution" to the loop word problem for $\mathcal{C}$. Namely, given a loop word w in the generators $\{\gamma_i\}$, w can be arranged into the normal form $z\gamma_1^r(\gamma_2^s(\gamma_3^t(\dots)))$ by simply powering, commuting, and associating elements, while keeping track of "error terms" with σ, χ, and α. Theorem 6.6 can then be interpreted as saying precisely that this solution is actually consistent, i.e., that we are never forced to kill Z.

In fact, this normal form procedure provides a method for doing calculations in any SFML. Furthermore, while building an SFML from 1-dimensional pieces becomes unwieldy for large dimension, by using larger associative (or at least familiar) pieces as building blocks, and gluing them together with the semidirect central product, it is not hard to do hand calculations in, say, 12- or 16-dimensional examples. See [15].

Remark 6.8. Conway (personal communication) has remarked that he and Parker orignally verified the existence of the Parker loop (unpublished) by proving a "consistency" theorem analogous to MacLane's theorems for monoidal categories [17, Ch. VII], using "pentagonal" and "hexagonal" relations in the Parker loop. This approach could also probably be used to prove Theorem 6.6.

Finally, we prove Main Theorem C.

Proof of Main Theorem C. Because of Theorems 6.1 and 6.6, it remains only to show that if L and M are SFML's, with distinguished central subgroups Z_L and Z_M, and associated CVS's C_L and C_M, and there is an isomorphism $\phi : L \to M$ such that $\phi(Z_L) = Z_M$, then C_L and C_M are isomorphic up to scalar multiple. However, since σ, χ, and α are only determined by the isomorphism type of an SFML, by choosing corresponding generators of Z_L and Z_M (i.e., by applying a scalar multiple), we can make C_L and C_M isomorphic. The theorem follows. $\square$

7. Isotopy in small Frattini Moufang 3-loops

In this section, as a fairly straightforward application of Main Theorem C, we characterize isotopy in SFML's. Now, because of Corollary 3.12, any SFM p-loop is a G-loop, unless $p = 3$. Therefore, even though much of what we say will apply in general, throughout this section, we assume that L is a finite SFM 3-loop, that Z is a fixed central subgroup of L, and that $C \cong L/Z$ is an elementary abelian 3-group. In other words, we assume that L is a coded extension of a CVS $(C, \sigma, \chi, \alpha)$ over $\mathbf{F}_3$. We also resume the convention that $\gamma, \delta, \epsilon, \kappa \in L$ reduce to $c, d, e, k \in C$.

Definition 7.1. Let L be a Moufang loop. For $\gamma, \delta, \kappa \in L$, we define

$$\gamma \circ_\kappa \delta = (\gamma\kappa)(\kappa^{-1}\delta). \tag{7.1}$$

It is easily verified that the set L and the operation $\circ_\kappa$ form a loop $(L, \circ_\kappa)$, with identity 1. Because (U, V, ι) is an isotopism from L to $(L, \circ_\kappa)$, where $U(x) = x\kappa^{-1}$, $V(x) = \kappa x$, and $\iota(x) = x$, $(L, \circ_\kappa)$ is called the *κ-isotope* of L.

Remark 7.2. Note that the di-associativity of L implies that for $\gamma \in L$, γ^{-1} is still the inverse of γ in $(L, \circ_\kappa)$.

We can now state the following fundamental result on isotopy in Moufang loops (see Pflugfelder [18, Thm. IV.4.1]).

Theorem 7.3. *If L is a Moufang loop, then any loop-isotope of L is isomorphic to a κ-isotope of L.* $\square$

The following formula therefore reduces isotopy in SFML's to a matter of multilinear algebra.

Theorem 7.4. *We have*

$$\gamma \circ_\kappa \delta = \gamma\delta \cdot \alpha(c,k,d). \tag{7.2}$$

Proof. Applying the multilinear and symplectic properties of α, we have:

$$\begin{aligned} \gamma \circ_\kappa \delta &= (\gamma\kappa)(\kappa^{-1}\delta) \\ &= \gamma(\kappa(\kappa^{-1}\delta)) \cdot \alpha(c,k,k^{-1}d) \\ &= \gamma\delta \cdot \alpha(c,k,d). \quad \square \end{aligned} \tag{7.3}$$

We now only need the following definitions to proceed.

Definition 7.5. The *radical* of α (resp. χ), denoted by $\mathrm{rad}(\alpha)$ (resp. $\mathrm{rad}(\chi)$), is the set of all $c \in C$ such that $\alpha(c,d,e) = 1$ (resp. $\chi(c,d) = 1$) for all $d, e \in C$ (resp. $d \in C$). Note that $\mathrm{rad}(\alpha) = N(L)/Z$ and $\mathrm{rad}(\chi) = C(L)/Z$.

Definition 7.6. Let $(C, \sigma(c), \chi(c,d), \alpha(c,d,e))$ be a CVS. For $k \in C$, the *adjoint translate* $\mathrm{adt}_k(C)$ is defined to be the CVS $(C, \sigma(c), \chi(c,d)\alpha(c,k,d), \alpha(c,d,e))$. The operation adt_k is called an *adjoint translation.*

In the following, we write $\gamma \circ_\kappa \delta$ as $\gamma \circ \delta$. Also, for $\gamma, \delta, \epsilon \in L$, we define $\gamma^{\circ n}$ inductively by $\gamma^{\circ 0} = 1$ and $\gamma^{\circ(n+1)} = \gamma \circ \gamma^{\circ n}$; we define $[\gamma, \delta]_\circ$ to be $(\delta \circ \gamma)^{-1}(\gamma \circ \delta)$; and we define $[\gamma, \delta, \epsilon]_\circ$ to be $(\gamma \circ (\delta \circ \epsilon))^{-1}((\gamma \circ \delta) \circ \epsilon)$. (See Remark 7.2.) Main Theorem D then comes from the following result.

Theorem 7.7. *We have the formulas*

$$\gamma^{\circ n} = \gamma^n, \tag{7.4}$$

$$[\gamma, \delta]_\circ = \chi(c,d)\alpha(c,k,d)^{-1}, \tag{7.5}$$

$$[\gamma, \delta, \epsilon]_\circ = \alpha(c,d,e). \tag{7.6}$$

In particular, $\gamma^{\circ 3} = \sigma(\gamma)$.

Proof. We first verify (7.4) by induction. Applying (7.2), we have

$$\gamma^{\circ(n+1)} = \gamma \circ \gamma^n = \gamma\gamma^n \cdot \alpha(c,k,c^n) = \gamma^{n+1}, \tag{7.7}$$

with the last equality following from the symplectic property of α. (7.4) follows.

Next, from (7.2) and

$$\delta \circ_\kappa \gamma = \delta\gamma \cdot \alpha(d,k,c), \tag{7.8}$$

it follows that

$$\begin{aligned} [\gamma, \delta]_\circ &= (\delta \circ \gamma)^{-1}(\gamma \circ \delta) \\ &= (\delta\gamma)^{-1}(\gamma\delta) \cdot \alpha(d,k,c)^{-1}\alpha(c,k,d) \\ &= [\gamma, \delta] \cdot \alpha(c,k,d)^2 \\ &= \chi(c,d)\alpha(c,k,d)^{-1}, \end{aligned} \tag{7.9}$$

with the last equality following because Z has exponent 3. (7.5) follows.

Finally, since

$$(\gamma \circ \delta) \circ \epsilon = (\gamma\delta)\epsilon \cdot \alpha(c,k,d)\alpha(cd,k,e) \tag{7.10}$$

$$\gamma \circ (\delta \circ \epsilon) = \gamma(\delta\epsilon) \cdot \alpha(d,k,e)\alpha(c,k,de), \tag{7.11}$$

we have that

$$\begin{aligned}[\gamma,\delta,\epsilon]_\circ &= (\gamma \circ (\delta \circ \epsilon))^{-1}((\gamma \circ \delta) \circ \epsilon)\\ &= [\gamma,\delta,\epsilon] \cdot \alpha(c,k,d)\alpha(cd,k,e)\alpha(d,k,e)^{-1}\alpha(c,k,de)^{-1}\\ &= \alpha(c,d,e)\alpha(c,k,d)\alpha(c,k,e)\alpha(d,k,e)\\ &\qquad \cdot \alpha(d,k,e)^{-1}\alpha(c,k,d)^{-1}\alpha(c,k,e)^{-1}\\ &= \alpha(c,d,e).\end{aligned} \tag{7.12}$$

The theorem follows. □

Proof of Main Theorem D. From (7.4)–(7.6), it follows that $(L, \circ_\kappa)$ is the coded extension of $\mathrm{adt}_{k^{-1}}(C)$, since condition 1 of Definition 4.9 follows from (7.5) and (7.6), and the formulas (4.10)–(4.12) of condition 2 of Definition 4.9 follow from the formulas (7.4)–(7.6), respectively. Therefore, any κ-isotope of L is a coded extension of an adjoint translate of C, and vice versa. The theorem follows. □

We illustrate Main Theorems C and D by enumerating the isomorphism and isotopy classes of the nonassociative coded extensions of the CVS's of dimension 3 and 4 over $\mathbf{F}_3$. For simplicity, we only discuss the exponent 3 ($\sigma = 1$) cases. In the following, we let $(C, 1, \chi, \alpha)$ be the CVS under discussion, we let L be its coded extension, and we let $Z = \langle \omega \rangle$.

Example 7.8. In the dimension 3 case, either $\chi = 1$ (i.e., L is commutative), or there exists a basis $\{k, c, d\}$ of C such that $\mathrm{rad}(\chi) = \langle k \rangle$ and $\chi(c, d) = \omega$. After possibly inverting k, we may assume that $\alpha(c, k, d) = \omega$, so there are two possibilities for L, up to isomorphism. However, in the non-commutative case, $\mathrm{adt}_k(C)$ has $\chi = 1$ as its bilinear form, so the two isomorphism classes are isotopic.

Example 7.9. In dimension 4, since we assume α is nontrivial, there is some $c \in C$ such that $c \notin \mathrm{rad}(\alpha)$. Therefore, since $\alpha(c, -, -)$ is a nontrivial bilinear symplectic form on C whose radical contains c, we may choose a basis $\{c, d, e, f\}$ for C such that $\alpha(c, d, -) = 1$ and $\alpha(c, e, f) = \alpha(d, e, f)^{-1}$. It may then be easily verified on the basis $\{c, d, e, f\}$ that $cd \in \mathrm{rad}(\alpha)$. Therefore, $\mathrm{rad}(\alpha)$ is 1-dimensional. It follows easily that α is unique up to isomorphism, and that we have four possible isomorphism classes for C (and therefore, for L):

1. χ trivial;
2. χ nondegenerate;
3. $\mathrm{rad}(\chi)$ 2-dimensional, containing $\mathrm{rad}(\alpha)$; and

4. $\operatorname{rad}(\chi)$ 2-dimensional, not containing $\operatorname{rad}(\alpha)$.

So now let $\operatorname{rad}(\alpha) = \langle c \rangle$. First, for $d \in C$, $\chi(c, d)$ is invariant under adjoint translation, so isomorphism classes 1 and 2 cannot be adjoint translates. Conversely, if χ is nondegenerate, without loss of generality, we may choose a basis $\{c, k, d, e\}$ for C such that $\langle c, k \rangle$ and $\langle d, e \rangle$ are orthogonal with respect to χ and $\chi(d, e) = \alpha(d, k, e)$, in which case $\operatorname{adt}_k(C)$ is in isomorphism class 4. On the other hand, if $\operatorname{rad}(\alpha) = \langle c \rangle$ and $\operatorname{rad}(\chi) = \langle c, k \rangle$, then by inverting k if necessary, we may choose a basis $\{c, k, d, e\}$ for C such that $\chi(d, e) = \alpha(d, k, e)$, in which case $\operatorname{adt}_k(C)$ is in isomorphism class 1. Therefore, we have precisely two isotopy classes: isomorphism classes 1 and 3, and isomorphism classes 2 and 4.

Compare Bénéteau [2, IV.3] and Ray-Chaudhuri and Roth [19].

8. A construction of all finite Moufang loops of class 2

In this section, we give a construction of all finite Moufang p-loops of class 2, which, because of Theorem 3.9, gives a construction of all finite Moufang loops of class 2. We will mostly be imitating Sections 4–7, using modules instead of vector spaces, so many details will be omittted.

Notation. For the rest of this section, we let p be a prime, we let L be a Moufang p-loop with a central subgroup Z such that $C \cong L/Z$ is an abelian group, and we resume our $\gamma, \delta, \epsilon, \dots$ and $c, d, e, \dots$ convention.

We would like to say that L gives C the structure of a "coded module," whatever that means. Now, χ and α work exactly as they do for SFML's (Theorem 3.3). However, if r is the exponent of Z, the only well-defined "power functions" $\sigma : C \to Z$ are the qth power functions, where r divides q, so if $r > p$, these power functions no longer capture all of the information we need. We fix this problem with the following definition.

Definition 8.1. A *coded module* is defined to be a 6-tuple $(C, Z, \{c_i\}, \{z_i\}, \chi, \alpha)$, where C and Z are finite abelian p-groups; $\{c_i\}$ is a basis (set of independent generators) for C; $\{z_i\}$ is a set of elements of Z; and $\chi : C \times C \to Z$ and $\alpha : C \times C \times C \to Z$ satisfy (3.6)–(3.9) and (3.10)–(3.13) for all $c, d, e, f \in C$ and all $n \in \mathbf{Z}$.

We then see that L, along with a choice of basis $\{c_i\}$ for C and a choice of preimages γ_i in L, makes C and Z into a coded module, by defining $z_i = \gamma_i^{q_i}$, where q_i is the order of c_i, and defining χ and α as usual.

We may now recover much of Sections 4 and 6 in the case of coded modules. First, we can generalize the definition of coded extension (Definition 4.9) to coded modules by removing the condition that Z have order p, and replacing (4.10) with

$$\gamma_i^{q_i} = z_i. \tag{8.1}$$

Imitating Theorem 4.10, we see that a loop L (with choice of preimages, etc.) is a coded extension of C if and only if L is a Moufang p-loop of class 2 whose coded module is C.

Having carried over the basic definitions, we next generalize the results of Section 6 appropriately. First, the uniqueness of coded extensions follows from the proof of Theorem 6.1, replacing (6.1) with (8.1), and (6.4) with defining (group) relations for Z. The definition of the semidirect central product (Definition 6.2) also still works, as does Theorem 6.3, if we replace the verification of (4.10) by the observation that concatenation of the bases of D and E produces a basis for C. Finally, coded extensions of 1-dimensional coded modules are easy to construct using central products of groups, so Theorem 6.6 follows as before.

In fact, in general, the only result not carried over from Section 6 is the "isomorphic SFML's implies isomorphic CVS's" statement of Main Theorem C, since the structure of a coded module is highly basis-dependent. However, if Z is elementary abelian, then by defining $\sigma_q(c) : C_q \to Z$ by $\sigma_q(c) = \gamma^q$, for all $q = p^n$, where C_q is the subgroup of C of all elements of C whose order divides q, we may actually recover all of Main Theorem C. In fact, since (4.2) holds in the elementary abelian case if we replace p with q, everything works as before. (In particular, when q is a power of 2, σ_q is linear for $q > 2$.)

We can also generalize Main Theorem D to the case where Z is an elementary abelian 3-group and C is a coded module with values in Z. We state this result in the following theorem, whose proof may be copied directly from Section 7. (Note that the proof of Theorem 7.7 only uses the exponent of Z, and not its order.)

Theorem 8.2. *Let L be a coded extension of a coded module C of 3-power order by an elementary abelian 3-group. Then up to isomorphism, the loop-isotopes of L are precisely the coded extensions of the adjoint translates of C. In particular, σ_q ($q = 3^n$) and α are "isotopy invariants" of L.* □

For example, Theorem 8.2 applies when L has exponent 3 and class 2.

Finally, we address the question analogous to the one posed in Section 5: that of which χ, α, etc., can be chosen for a coded module. (The 1-dimensional case shows that any values may be chosen for the z_i.) Again, for $p > 2$, this is easy (keeping in mind that $\alpha^6 = 1$), so it will be enough to prove Theorem 8.3, in which we use the following conventions.

Notation. We revert to additive notation for abelian groups. All summations, indices, etc., are from 1 to n in the manner indicated. (For instance, $i < j$ means for all $1 \leq i < j \leq n$.) We also let $\alpha_{ijk} = \alpha(x_i, x_j, x_k)$.

Theorem 8.3. *Let C and Z be finite abelian 2-groups, and let $\{x_i\}$ be a basis for C. Choose some symplectic multilinear function $\alpha : C \times C \times C \to Z$ such that $2\alpha = 0$ identically, and for all i, j, choose $\chi_{ij} \in Z$ such that:*

1. $\chi_{ii} = 0$,
2. $\chi_{ij} = -\chi_{ji}$, *and*
3. *the (additive) order of* χ_{ij} *divides the order of* x_i.

Let $c = \sum_i c_i x_i$ *and* $d = \sum_j d_j x_j$. *The function* $\chi : C \times C \to Z$ *defined by*

$$\chi(c, d) = \sum_{i \neq j} c_i d_j \chi_{ij} + \sum_{i<j} \sum_k c_i c_j d_k \alpha_{ijk} + \sum_i \sum_{j<k} c_i d_j d_k \alpha_{ijk}, \tag{8.2}$$

along with any choice of elements $z_i \in Z$, *gives* C *the structure of a coded module. Furthermore, any even coded module may be constructed in this way.*

Note that the first term of the right-hand side of (8.2) makes sense only when condition 3 is satisfied, since the c_i in $c = \sum_i c_i x_i$ is only well-defined as an integer mod the order of x_i. Also, the last two terms of (8.2) are invariant under a reordering of the basis only because α_{ijk} is symmetric in all three indices.

Proof. Given a coded module, if $\chi_{ij} = \chi(x_i, x_j)$, then conditions 1, 2, and 3 follow from (3.6), (3.7), and Theorem 3.7, respectively. Furthermore, (8.2) follows from repeated application of (3.9) and (3.13), and $2\alpha = 0$ follows from Main Theorem A. Our last assertion follows easily.

As for the first assertion, it suffices to check (3.6)–(3.9); in fact, because of (3.14), it suffices to check (3.6), (3.7), and (3.9). In the following, let $c = \sum_i c_i x_i$, $d = \sum_i d_i x_i$, and $e = \sum_i e_i x_i$.

To check (3.6), we compute

$$\begin{aligned}
\chi(c, c) &= \sum_{i \neq j} c_i c_j \chi_{ij} + \sum_{i<j} \sum_k c_i c_j c_k \alpha_{ijk} + \sum_i \sum_{j<k} c_i c_j c_k \alpha_{ijk} \\
&= \sum_{i<j} (c_i c_j \chi_{ij} + c_j c_i \chi_{ji}) + \sum_{i<j} \sum_k c_i c_j c_k \alpha_{ijk} + \sum_{j<k} \sum_i c_j c_k c_i \alpha_{jki} \\
&= 0,
\end{aligned} \tag{8.3}$$

since $\chi_{ij} + \chi_{ji} = 0$, $\alpha_{jki} = \alpha_{ijk}$, and $2\alpha = 0$.

To check (3.7), we compute

$$\begin{aligned}
\chi(c, d) &= \sum_{i \neq j} c_i d_j \chi_{ij} + \sum_{i<j} \sum_k c_i c_j d_k \alpha_{ijk} + \sum_i \sum_{j<k} c_i d_j d_k \alpha_{ijk} \\
&= -\sum_{j \neq i} d_j c_i \chi_{ji} + \sum_{j<k} \sum_i d_j d_k c_i \alpha_{jki} + \sum_k \sum_{i<j} d_k c_i c_j \alpha_{kij} \\
&= -\chi(d, c),
\end{aligned} \tag{8.4}$$

since $\chi_{ij} = -\chi_{ji}$, $\alpha_{jki} = \alpha_{kij} = \alpha_{ijk}$, and $\alpha = -\alpha$.

Finally, to check (3.9), we compute

$$
\begin{aligned}
\chi(c+d,e) &= \sum_{i\neq j}(c_i+d_i)e_j\chi_{ij} + \sum_{i<j}\sum_{k}(c_i+d_i)(c_j+d_j)e_k\alpha_{ijk} \\
&\quad + \sum_{i}\sum_{j<k}(c_i+d_i)e_je_k\alpha_{ijk} \\
&= \sum_{i\neq j} c_ie_j\chi_{ij} + \sum_{i\neq j} d_ie_j\chi_{ij} \\
&\quad + \sum_{i<j}\sum_{k} c_ic_je_k\alpha_{ijk} + \sum_{i<j}\sum_{k} d_id_je_k\alpha_{ijk} \\
&\quad + \sum_{i}\sum_{j<k} c_ie_je_k\alpha_{ijk} + \sum_{i}\sum_{j<k} d_ie_je_k\alpha_{ijk} \\
&\quad + \sum_{i<j}\sum_{k} c_id_je_k\alpha_{ijk} + \sum_{i<j}\sum_{k} d_ic_je_k\alpha_{ijk} \\
&= \chi(c,e) + \chi(d,e) + \alpha(c,d,e),
\end{aligned} \tag{8.5}
$$

since

$$
\begin{aligned}
&\sum_{i<j}\sum_{k} c_id_je_k\alpha_{ijk} + \sum_{i<j}\sum_{k} d_ic_je_k\alpha_{ijk} \\
&= \sum_{i<j}\sum_{k} c_id_je_k\alpha_{ijk} + \sum_{i>j}\sum_{k} c_id_je_k\alpha_{ijk} \\
&= \alpha(c,d,e),
\end{aligned} \tag{8.6}
$$

using $\alpha_{ijk} = \alpha_{jik}$ and $\alpha_{kjk} = \alpha_{ikk} = 0$. The theorem follows. □

Finally, when Z is an elementary abelian p-group, we have seen previously that it is possible to define $\sigma_q : C_q \to Z$ for all $q = p^n$, and so the problem arises of which values can be chosen for σ_q. Now, since σ_q is trivial on $C_{q/p}$, for $q > 2$, we may choose σ_q freely on a basis for $C_q/C_{q/p}$, since σ_q is linear for $q > 2$. Therefore, the only case remaining is $\sigma = \sigma_2$. We leave it to the interested reader to verify (by imitating the proof of Theorem 8.3) that if we choose arbitrary elements $\sigma_i \in Z$, and define

$$
\sigma(c) = \sum_{i} c_i\sigma_i + \sum_{i<j} c_ic_j\chi_{ij} + \sum_{i<j<k} c_ic_jc_k\alpha_{ijk}, \tag{8.7}
$$

then σ has the desired properties.

Remark 8.4. Note that since our results, in most cases, say nothing about the isomorphism problem for Moufang loops of class 2, the result in group theory which is probably closest to our construction is the fact that every nilpotent group has a consistent polycyclic presentation. For more about polycyclic presentations, see Sims [21, 9.4].

9. Acknowledgements

The author was partly supported by a University of Michigan Rackham Summer Faculty Fellowship, and by the generosity of MSRI and its staff. (Research at MSRI is supported in part by NSF grant DMS-9022140.) The author would also like to thank J. H. Conway and L. Schneps for their helpful remarks. Extraspecial thanks goes to R. L. Griess for making many helpful comments on an early draft of this paper, and for considerable help in formulating Definition 4.3 and proving Theorem 4.4.

References

[1] M. Aschbacher, *Finite group theory*, Cambridge Univ. Press, 1986.
[2] L. Bénéteau, *Commutative Moufang loops and related groupoids*, In Chein et al. [7], pp. 115–142.
[3] R. H. Bruck, *Contributions to the theory of loops*, Trans. AMS **60** (1946), 245–354.
[4] ———, *Some theorems on Moufang loops*, Math. Z. **73** (1960), 59–78.
[5] ———, *A survey of binary systems*, Ergebnisse der Mathematik und ihrer Grenzgebiete, vol. 20, Springer-Verlag, New York, 1971.
[6] O. Chein, *Examples and methods of construction*, In Chein et al. [7], pp. 27–93.
[7] O. Chein, H. O. Pflugfelder, and J. D. H. Smith (eds.), *Quasigroups and loops: Theory and applications*, Sigma Series in Pure Mathematics, vol. 8, Berlin, Heldermann Verlag, 1990.
[8] J. H. Conway, *A simple construction for the Fischer-Griess monster group*, Invent. Math. **79** (1985), 513–540.
[9] J. H. Conway, R. T. Curtis, S. P. Norton, R. A. Parker, and R. A. Wilson, *ATLAS of finite groups*, Oxford Univ. Press, 1985.
[10] T. Evans, *Varieties of loops and quasigroups*, In Chein et al. [7], pp. 1–26.
[11] G. Glauberman, *On loops of odd order II*, J. Alg. **8** (1968), 393–414.
[12] G. Glauberman and C. R. B. Wright, *Nilpotence of finite Moufang 2-loops*, J. Alg. **8** (1968), 415–417.
[13] R. L. Griess, *Code loops*, J. Alg. **100** (1986), 224–234.
[14] ———, *Sporadic groups, code loops, and nonvanishing cohomology*, J. Pure Appl. Alg. **44** (1987), 191–214.
[15] T. Hsu, *Explicit constructions of code loops via semidirect central products*, in preparation, 1996.
[16] Masaaki Kitazume, *Code loops and even codes over F_4*, J. Alg. **118** (1988), 140–149.
[17] S. MacLane, *Categories for the working mathematician*, Springer-Verlag, New York, 1971.
[18] H. O. Pflugfelder, *Quasigroups and loops: Introduction*, Sigma Series in Pure Mathematics, vol. 7, Heldermann Verlag, Berlin, 1990.
[19] D. K. Ray-Chaudhuri and R. Roth, *Hall triple systems and commutative Moufang exponent 3 loops: The case of nilpotence class 2*, J. Comb. Thy. (A) **36** (1984), 129–162.
[20] T. M. Richardson, *Local subgroups of the Monster and odd code loops*, Trans. AMS **347** (1995), no. 5, 1453–1531.
[21] C. C. Sims, *Computation with finitely presented groups*, Cambridge Univ. Press, 1994.
[22] J. D. H. Smith, *A second grammar of associators*, Math. Proc. Cam. Phil. Soc. **84** (1978), 405–415.

[23] ———, *Combinatorial characters of quasigroups*, Coding Theory and Design Theory (D. Ray-Chaudhuri, ed.), IMA Vols. in Math. and its Appls., vol. 20, Springer-Verlag, New York, 1990, pp. 163–187.

Department of Mathematics, University of Michigan, Ann Arbor, MI 48109
E-mail address: `timhsu@@math.lsa.umich.edu`