FACULTY OF MATHEMATICS AND PHYSICS
CHARLES UNIVERSITY

Department of Algebra

CONNECTIONS BETWEEN CODES, GROUPS AND LOOPS

Doctoral thesis

Petr Vojtěchovský

Advisor: doc. Aleš Drápal, CSc.

Branch M2-Algebra

PRAHA 2003

With thanks to Aleš Drápal and Jonathan D. H. Smith

Contents

Chapter 1

Introduction

This work grew out of a series of papers written by the author, sometimes in cooperation with others, mostly in the period 2000–2002. See [13], [24], [37], [42], [43], [52], [53], [54], [55], [56], [57], [58], [59], [60], [61].

As the title reveals, the connections between codes, groups and loops form the central theme of this thesis.

Each chapter can be read independently once the reader becomes familiar with the notation and terminology gathered below. On the other hand, although each chapter is based on one or two papers, some effort was made to present the entire work in a uniform way.

A typical chapter starts with the summary of results that will be proved in it. Definitions not given in this introduction are provided when needed.

It was our intention to avoid most of the results that appeared already in [55]—the doctoral thesis written under the supervision of Jonathan D. H. Smith at Iowa State University. Nevertheless some overlap exists. For instance, sections 3.2 and 4.1 are taken from [55].

1.1 Notation and terminology

A set equipped with one binary operation $\cdot$ is called a *groupoid* (or, sometimes, *binar* or *magma*). We often write ab instead of $a \cdot b$. It is handy to use $\cdot$ instead of parentheses to indicate the order in which elements are going to be multiplied. For instance, $a \cdot bc$ stands for $a(bc)$, and $a \cdot (bc \cdot d)$ stands for $a((bc)d)$.

If Q is a groupoid in which the equation $xy = z$ has a unique solution in Q whenever two of the three elements x, y, $z \in Q$ are given, it is called a *quasigroup*. Multiplication tables of finite quasigroups are known in combinatorics as *Latin squares*.

If Q is a quasigroup containing an element 1 such that $1x = x1 = x$ holds for every $x \in Q$, then Q is called a *loop*, and 1 is the (unique) *neutral element* of Q.

Given an element x of a loop Q, there is a unique $y \in Q$ such that $xy = 1$. If Q is associative, we have $x \cdot yx = xy \cdot x = 1 \cdot x = x$. Since $x \cdot 1 = x$ is also satisfied,

we must have $yx = 1$. In other words, if Q is an associative loop then every element $x \in Q$ has a *two-sided inverse* x^{-1} such that $xx^{-1} = x^{-1}x = 1$. Associative loops are therefore exactly *groups*. There are loops Q that are not associative yet posses a two-sided inverse x^{-1} for every $x \in Q$.

Assume that Q is a quasigroup. 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 $(xy)z = x(yz) \cdot [x, y, z]$.

The set $C(Q) = \{x;\ xy = yx \text{ for every } y \in Q\}$ is called the *commutant* of Q. It is often called the *Moufang center*. The *left* (resp. *middle*, *right*) *nucleus* of Q consists of all elements $x \in Q$ such that $xy \cdot z = x \cdot yz$ (resp. $yx \cdot z = y \cdot xz$, $yz \cdot x = y \cdot zx$). It is denoted by $N_\lambda(Q)$ (resp. $N_\mu(Q)$, $N_\rho(Q)$). The intersection $N(Q) = N_\lambda(Q) \cap N_\mu(Q) \cap N_\rho(Q)$ is the *nucleus* of Q. The *center* of Q is then $Z(Q) = C(Q) \cap N(Q)$, i.e., the center consists of all elements that commute and associate with all elements of Q.

The permutation group $\mathrm{Aut}(Q)$ consisting of all automorphisms of Q is called the *automorphism group* of Q.

Every element $x \in Q$ defines two permutations of Q, $L_x : y \mapsto xy$ and $R_x : y \mapsto yx$, called the *left translation by* x and *right translation by* x, respectively. Unlike in groups, a composition of two translations of the same kind is not necessarily a translation. The permutation group $\mathrm{Mlt}(Q)$ generated by all left and right translations of Q is known as the *multiplication group* of Q. The *left* (resp. *right*) *multiplication group* $\mathrm{LMlt}(Q)$ (resp. $\mathrm{RMlt}(Q)$) of Q is the group generated by all left (resp. right) translations of Q.

Assume that Q is a loop. The subgroup $\mathrm{Inn}(Q)$ of $\mathrm{Mlt}(Q)$ consisting of all permutations fixing 1 is called the *inner mapping group* of Q. A subset S of Q is a *subloop* of Q if it is closed under multiplication and contains the neutral element of Q. We write $S \leq Q$. A subloop S of Q is *normal* in Q if it is closed under the action of $\mathrm{Inn}(Q)$, and we write $S \trianglelefteq Q$.

When Q is a loop, both $N(Q)$ and $Z(Q)$ are subgroups of Q. Moreover, $Z(Q)$ is always normal in Q. The *associator subloop* $A(Q)$ of Q generated by all associators $[x, y, z]$ with x, y, $z \in Q$ is another normal subloop of Q.

Many classes of loops are defined by *near-associativity* identities. For example, every loop Q satisfying the identity $x(y(xz)) = (x(yx))z$ is a *left Bol loop*. Similarly, *right Bol loops* are loops satisfying $((xy)z)y = x((yz)y)$. *Moufang loops* are loops that are both left Bol and right Bol. Equivalently, a loop is Moufang if it satisfies the identity $x(y(xz)) = ((xy)x)z$.

If the subloop generated by any element of Q is a subgroup then Q is said to be *power associative*. In a finite power associative loop Q, it makes sense to define the *order* of x as the smallest positive integer n such that $x^n = 1$. If the subloop generated by any two elements of Q is a subgroup then Q is said to be *diassociative*. Bol loops are power associative. Moufang loops are diassociative, hence power associative. Every element x of a Moufang loop is accompanied by its two-sided inverse x^{-1}.

Chapter 2

Combinatorial Polarization

Combinatorial polarization is a process similar to the principle of inclusion and exclusion. We first study combinatorial polarization over finite fields, and then connect it to an important class of Moufang loops, called code loops. Code loops are precisely finite Moufang loops that posses at most two squares. Every code loop can be identified with a 3rd derived form of a map of combinatorial degree 3. In order to see this, one must show how to construct a doubly even binary code with prescribed Hamming weights of intersections of codewords. We generalize this construction to binary codes of level $r \geq 2$. We also indicate how combinatorial designs come into play, although the full picture is not clear yet.

2.1 Derived forms

Let F be a field and V a vector space over F. Let $f : V \longrightarrow F$ be an arbitrary map. Then the sth *derived form* of f is the map $\delta_s f : V^s \longrightarrow F$ defined by

$$\delta_s f(v_1, \ldots, v_s) = \sum_{\emptyset \neq \{i_1, \ldots, i_r\} \subseteq \{1, \ldots, s\}} (-1)^{s-r} f(v_{i_1} + \cdots + v_{i_r}), \tag{2.1}$$

for every $v_1, \ldots, v_s \in V$. If the number of arguments is clear from the context, we will write δf instead of $\delta_s f$.

It is obvious from the definition that δf is symmetric with respect to all arguments. Since the arguments of δf do not have to be distinct, we will find it convenient to consider collections of vectors rather than sets of vectors. Nevertheless, we shall denote collections in the same way as sets; e.g., $A = \{u, v, v\}$ is a collection of three vectors, and $A \cup A = \{u, v, v, u, v, v\}$, say.

Let $A = \{v_1, \ldots, v_s\}$ be a collection of vectors. Let us write $\sum A$ for $v_1 + \cdots + v_s$ and $\delta f(A)$ for $\delta f(v_1, \ldots, v_s)$. Then the defining equation (2.1) can be restated as

$$\delta f(A) = \sum_{B \subseteq A} (-1)^{|A|-|B|} f(\sum B),$$

if we agree that $f(\sum \emptyset) = 0$.

As we are going to show, every derived form can be calculated using the recursive formula

$$\delta_{s+1}f(\{v_1, v_2\} \cup A) = \delta_s f(\{v_1 + v_2\} \cup A) - \delta_s f(\{v_1\} \cup A) - \delta_s f(\{v_2\} \cup A), \quad (2.2)$$

where A is a collection of $s-1$ vectors. This formula is known as *polarization*, and we usually say that $\delta_s f$ and $\delta_{s+1} f$ are *related by polarization.*

Lemma 2.1 *Let F be a field, V a vector space over F and $f : V \longrightarrow F$ a map. Then f satisfies* (2.2) *for every $s \geq 1$.*

Proof. Let $m = s + 1$. Fix a collection $B \subseteq A$ and count how many times the expression $f(\sum B)$ appears on the right hand side of (2.2). If v_1, $v_2 \in B$, it appears only in $\delta_s f(\{v_1+v_2\}\cup A)$, namely with the sign $(-1)^{s-(|B|-1)} = (-1)^{m-|B|}$. If $v_1 \in B$ and $v_2 \notin B$, it only appears in $\delta_s f(\{v_1\} \cup A)$ with the sign $-(-1)^{s-|B|} = (-1)^{m-|B|}$. Similarly when $v_2 \notin B$ and $v_1 \in B$. Finally, if v_1, $v_2 \notin B$, $f(\sum B)$ is counted three times with the signs $(-1)^{s-|B|} - (-1)^{s-|B|} - (-1)^{s-|B|} = (-1)^{m-|B|}$. Since the sign of $f(\sum B)$ in the definition (2.1) of $\delta_{s+1} f$ is $(-1)^{m-|B|}$, we are done. □

2.2 Combinatorial degree

Assume that V is an n-dimensional vector space over F, and that $f : V \longrightarrow F$ is an arbitrary map.

The *combinatorial degree* $\operatorname{cdeg} f$ of f is the smallest integer r such that $\delta_s f = 0$ for every $s > r$, if it exists, and it is equal to ∞ otherwise. Note that the zero map has combinatorial degree 0.

The polarization identity (2.2) shows that if $\delta_s f$ is the zero map, then $\delta_{s+t} f$ is the zero map for every $t \geq 0$. Hence the combinatorial degree is finite as long as $\delta_s f$ is the zero map for some s. This does not have to happen, though.

Lemma 2.2 *Let $f : V \longrightarrow F$ be a map. Then*

$$\delta_s f(0, \ldots, 0) = (-1)^{s+1} f(0).$$

In particular, $\operatorname{cdeg} f = \infty$ *when $f(0) \neq 0$.*

Proof. We have $\delta_1 f(0) = f(0) = (-1)^2 f(0)$. Assume that $\delta_s f(0, \ldots, 0)$ is equal to $(-1)^{s+1} f(0)$. Then

$$\delta_{s+1} f(0, \ldots, 0) = \delta_s f(0, \ldots, 0) - \delta_s f(0, \ldots, 0) - \delta_s f(0, \ldots, 0) = (-1)^{s+2} f(0),$$

by (2.2). □

For the rest of this section, suppose that $F = GF(q)$ is a finite field of characteristic p. Then, as is well-known, every $f : V \longrightarrow F$ coincides as a function with some polynomial in n variables $x_1, \ldots, x_n$ over F. Indeed, the interpolation polynomial

$$L(x_1, \ldots, x_n) = \sum_{a=(a_1,\ldots,a_n)\in V} f(a) \prod_{i=1}^{n} \prod_{b_i \neq a_i} \frac{x_i - b_i}{a_i - b_i} \quad (2.3)$$

does the job.

We will further assume that $f \in F[x_1, \ldots, x_n]$ is a *reduced polynomial*, which means that all monomials with the same multiexponent are summed up into one monomial, and that every exponent appearing in f belongs to $\{0, \ldots, q-1\}$. We loose no functions in this way, since $F^* = F \setminus 0$ is a cyclic group of order $q-1$, and thus $a^q = a$ holds for every $a \in F$. In fact, reduced polynomials are in one-to-one correspondence with functions $V \longrightarrow F$, as we will see in Lemma 2.3.

Every reduced polynomial f is a sum of monomials $cx_1^{a_1} \cdots x_n^{a_n}$, where $c \in F$ depends on the multiexponent $(a_1, \ldots, a_n)$, and where each a_i is in $\{0, \ldots, q-1\}$. Let us write $\mathbf{a}$ for the multiexponent $(a_1, \ldots, a_n)$, $\mathbf{x}$ for the n variables $(x_1, \ldots, x_n)$, and $\mathbf{x}^\mathbf{a}$ for the monomial $x_1^{a_1} \cdots x_n^{a_n}$. Let $M(f)$ be the set of all multiexponents of f. Then f can be conveniently expressed as

$$f(\mathbf{x}) = \sum_{\mathbf{a} \in M(f)} c_\mathbf{a} \mathbf{x}^\mathbf{a}, \tag{2.4}$$

where $c_\mathbf{a}$ is a constant from F^*. The *degree* of f is defined as

$$\deg f = \max_{(a_1,\ldots,a_n) \in M(f)} \sum_{i=1}^{n} a_i.$$

Every nonnegative integer m determines uniquely the coefficients $0 \le m_i \le p-1$ of its p-ary expansion $m = \sum_{i=0}^{\infty} m_i p^i$. The *$p$-weight* of m is the integer

$$w_p(m) = \sum_{i=0}^{\infty} m_i.$$

We consequently define the *p-degree* of f as

$$\deg_p f = \max_{(a_1,\ldots,a_n) \in M(f)} \sum_{i=1}^{n} w_p(a_i).$$

Note that $\deg_p f$ depends on $F = GF(q)$, not only on the characteristic p. Also note that $\deg f = \deg_p f$ when $p = q$, since then $w_p(a) = a$ for every reduced exponent a.

Lemma 2.3 *Assume that $F = GF(q)$ and that $f \in F[\mathbf{x}]$ is a reduced polynomial. Then f is the zero function $V = F^n \longrightarrow F$ if and only if f is the zero polynomial.*

Proof. Assume that f is not the zero polynomial. We want to show that f is not the zero function.

When $n = 1$, then f is a polynomial in one variable with $\deg f < q$. By the fundamental theorem of algebra, f has at most $\deg f$ roots, and thus there is $a \in F$ such that $f(a) \neq 0$.

Assume that $n > 1$, that the lemma holds for every polynomial in at most $n-1$ variables, and that all variables $x_1, \ldots, x_n$ appear in f. Then $f(\mathbf{x}) =$

$\sum_{i=0}^{m} x_1^i f_i(x_2, \ldots, x_n)$, for some polynomials $f_i \in F[x_2, \ldots, x_n]$ and integer $m < q$ such that f_m is not the zero polynomial. By the induction hypothesis, there is $(c_2, \ldots, c_n) \in F^{n-1}$ such that $f_m(c_2, \ldots, c_n) \neq 0$, say. Then $g(x_1) = f(x_1, c_2, \ldots, c_n)$ is a nonzero polynomial in one variable of degree $m < q$. By the fundamental theorem of algebra, there is $c_1 \in F$ such that $g(c_1) = f(c_1, \ldots, c_n) \neq 0$.

The other implication is trivial. □

We will therefore restrict our attention to reduced polynomials.

Two polynomials $f, g \in F[\mathbf{x}]$ are said to be *disjoint* if $M(f) \cap M(g) = \emptyset$.

Lemma 2.4 *Suppose that $f, g \in F[\mathbf{x}]$ are disjoint polynomials. Then $\delta_s f$, $\delta_s g$ are disjoint, too, for every $s \geq 1$.*

Proof. Since every polynomial is a sum of its monomials, it suffices to prove that if two monomials are disjoint (i.e., they have different multiexponents), their derived forms are disjoint.

Let $f(\mathbf{x_1}) = \mathbf{x_1}^{\mathbf{a}}$, where $\mathbf{x_1} = (x_{11}, \ldots, x_{1n})$ and $\mathbf{a} = (a_1, \ldots, a_n)$. The typical summand in (2.1) is $h = f(\mathbf{x_1} + \cdots + \mathbf{x_r})$, which is a polynomial in nr variables. The crucial observation is that for every $0 < j \leq r$, every monomial of h contains exactly a_i variables x_{ji}, with possible repetitions. Hence the original monomial $f(\mathbf{x_1})$ is uniquely determined by every monomial of h. □

Corollary 2.5 *Let $f \in F[\mathbf{x}]$. Then* $\operatorname{cdeg} f = \max_{\mathbf{a} \in M(f)} \operatorname{cdeg} \mathbf{x}^{\mathbf{a}}$.

From now on, we focus on reduced monomials.

When $\mathbf{a} = (a_1, \ldots, a_n)$ and $\mathbf{b} = (b_1, \ldots, b_n)$ are two multiexponents, we write $\mathbf{a} \leq \mathbf{b}$ if and only if $a_i \leq b_i$ for every $1 \leq i \leq n$, and $\mathbf{a} < \mathbf{b}$ if $\mathbf{a} \leq \mathbf{b}$ and $\mathbf{a} \neq \mathbf{b}$. Let $\mathbf{0}$ be the multiexponent $(0, \ldots, 0)$.

Lemma 2.6 *Let $f(\mathbf{x}) = \mathbf{x}^{\mathbf{a}}$. Then*

$$\delta_2 f(\mathbf{x}, \mathbf{y}) = \sum_{\mathbf{0} < \mathbf{b} < \mathbf{a}} c_{\mathbf{a},\mathbf{b}} \mathbf{x}^{\mathbf{b}} \mathbf{y}^{\mathbf{a}-\mathbf{b}}, \tag{2.5}$$

where

$$c_{\mathbf{a},\mathbf{b}} = \prod_{i=1}^{n} \binom{a_i}{b_i}. \tag{2.6}$$

Proof. We have

$$\begin{aligned}
(\mathbf{x}+\mathbf{y})^{\mathbf{a}} &= \prod_{i=1}^{n} (x_i + y_i)^{a_i} = \prod_{i=1}^{n} \sum_{b_i=0}^{a_i} \binom{a_i}{b_i} x_i^{b_i} y_i^{a_i - b_i} \\
&= \sum_{b_1, \ldots, b_n,\, 0 \leq b_i \leq a_i} \left(\prod_{i=1}^{n} \binom{a_i}{b_i} x_i^{b_i} y_i^{a_i - b_i} \right) \\
&= \sum_{b_1, \ldots, b_n,\, 0 \leq b_i \leq a_i} \left(\prod_{i=1}^{n} \binom{a_i}{b_i} \right) x_1^{b_1} \cdots x_n^{b_n} y_1^{a_1 - b_1} \cdots y_n^{a_n - b_n}.
\end{aligned}$$

Since $\delta_2 f(\mathbf{x}, \mathbf{y}) = (\mathbf{x}+\mathbf{y})^{\mathbf{a}} - \mathbf{x}^{\mathbf{a}} - \mathbf{y}^{\mathbf{a}}$, we are done. □

Remark 2.7 Equation (2.5) shows that $\delta_2 f$ is disjoint from $\delta_2 g$ whenever $f(\mathbf{x}) = \mathbf{x}^{\mathbf{a}}$, $g(\mathbf{x}) = \mathbf{x}^{\mathbf{c}}$, and $\mathbf{a} \neq \mathbf{c}$. Indeed, neglecting the constant, every monomial in $\delta_2 f$ is of the form $r = \mathbf{x}^{\mathbf{b}}\mathbf{y}^{\mathbf{a}-\mathbf{b}}$ with $\mathbf{0} < \mathbf{b} < \mathbf{a}$, by (2.5). Similarly, every monomial in $\delta_2 g$ is of the form $s = \mathbf{x}^{\mathbf{d}}\mathbf{y}^{\mathbf{c}-\mathbf{d}}$. It is obvious that $r = s$ if and only if $\mathbf{b} = \mathbf{d}$ and $\mathbf{a} - \mathbf{b} = \mathbf{c} - \mathbf{d}$. This implies that $\mathbf{a} = \mathbf{c}$.

Unfortunately, repeated application of δ only yields the 2^rth derived forms. One must therefore proceed as in Lemma 2.4 to prove that any two disjoint polynomials yield disjoint derived forms.

For the sake of brevity, let us identify the multiexponent $\mathbf{a}$ with the monomial $\mathbf{x}^{\mathbf{a}}$.

Lemma 2.8 *Let* $\mathbf{a_1}$ *be a multiexponent. Then*

$$\delta_s \mathbf{a_1}(\mathbf{x_1}, \ldots, \mathbf{x_2}) = \sum_{\mathbf{0<a_2<a_1}} \cdots \sum_{\mathbf{0<a_s<a_{s-1}}} c_{\mathbf{a_1},\mathbf{a_2}} \cdots c_{\mathbf{a_{s-1}},\mathbf{a_s}} \mathbf{x_1}^{\mathbf{a_s}} \mathbf{x_2}^{\mathbf{a_{s-1}}-\mathbf{a_s}} \cdots \mathbf{x_s}^{\mathbf{a_1}-\mathbf{a_2}}, \quad (2.7)$$

where $c_{\mathbf{a_i},\mathbf{a_{i+1}}}$ *is analogous to* (2.6).

Proof. By Lemma 2.6, the statement holds for $s = 2$. We proceed by induction on s. Assume that (2.7) holds for s. Using the polarization formula (2.2) on every summand of (2.7), we see that $\delta_{s+1}\mathbf{a_1}(\mathbf{x_1}, \ldots, \mathbf{x_{s+1}})$ is equal to

$$\sum_{\mathbf{0<a_2<a_1}} \cdots \sum_{\mathbf{0<a_s<a_{s-1}}} c_{\mathbf{a_1},\mathbf{a_2}} \cdots c_{\mathbf{a_{s-1}},\mathbf{a_s}} \delta_2 \mathbf{a_s}(\mathbf{x_1}, \mathbf{x_2}) \mathbf{x_3}^{\mathbf{a_{s-1}}-\mathbf{a_s}} \cdots \mathbf{x_{s+1}}^{\mathbf{a_2}-\mathbf{a_1}}.$$

By (2.5), the term $\delta_2 \mathbf{a_s}(\mathbf{x_1}, \mathbf{x_2})$ expands as

$$\sum_{\mathbf{0<a_{s+1}<a_s}} c_{\mathbf{a_s},\mathbf{a_{s+1}}} \mathbf{x_1}^{\mathbf{a_{s+1}}} \mathbf{x_2}^{\mathbf{a_s}-\mathbf{a_{s+1}}},$$

and we are through. □

Let $\mathbf{a} = (a_1, \ldots, a_n)$ be a multiexponent. Lemma 2.8 shows that $\delta_s \mathbf{a}$ is not the zero map if and only if there is a chain of multiexponents $\mathbf{a} = \mathbf{a_1} > \mathbf{a_2} > \cdots > \mathbf{a_s}$ such that $c_{\mathbf{a_i},\mathbf{a_{i+1}}}$ does not vanish in F for every $1 \leq i < s$. We will call such chains *regular* here. Obviously, the length of a regular chain is bounded by q^n.

Lemma 2.9 *Let* $\mathbf{a_i} = (a_{i1}, \ldots, a_{in})$*, for* $1 \leq i \leq s$*. Assume that* $\mathbf{a_1} > \cdots > \mathbf{a_s}$ *is a regular chain of maximum length for* $\mathbf{a_1}$*. Then* $\mathbf{a_{i+1}}$*,* $\mathbf{a_i}$ *differ in exactly one position, i.e.,* $a_{i+1,j} \neq a_{ij}$ *for a unique* $1 \leq j \leq n$*.*

Proof. Suppose that there are i, j, k with $1 \le i < s$ and $1 \le j < k \le n$ such that $a_{i+1,j} \ne a_{i,j}$ and $a_{i+1,k} \ne a_{i,k}$. Construct a multiexponent $\mathbf{b}$ according to

$$b_{i,m} = \begin{cases} a_{i,m}, & \text{if } m \ne j, \\ a_{i+1,m}, & \text{if } m = j. \end{cases}$$

Then $\mathbf{a_i} > \mathbf{b} > \mathbf{a_{i+1}}$. Since $c_{\mathbf{a_i},\mathbf{a_{i+1}}} = \prod_{m=1}^{n} \binom{a_{i,m}}{a_{i+1,m}} \ne 0$, we have $c_{\mathbf{a_i},\mathbf{b}} \ne 0$ and $c_{\mathbf{b},\mathbf{a_{i+1}}} \ne 0$. Thus $\mathbf{a_1}$, …, $\mathbf{a_i}$, $\mathbf{b}$, $\mathbf{a_{i+1}}$, …, $\mathbf{a_s}$ is a regular chain of length $s+1$, a contradiction. □

Corollary 2.10 *Let* $\mathbf{a} = (a_1, \ldots, a_n)$ *be a multiexponent,* $f(\mathbf{x}) = \mathbf{x}^{\mathbf{a}}$*, and* $f_i(x) = x^{a_i}$*,* $1 \le i \le n$*. Then*

$$\operatorname{cdeg} f = \sum_{i=1}^{n} \operatorname{cdeg} f_i.$$

We therefore continue to investigate combinatorial degrees of reduced monomials in one variable.

It is well-known (and easy to prove) that all binomial coefficients

$$\binom{n}{k} = \frac{n!}{(n-k)!k!}$$

can be found in the *Pascal triangle*, which is an infinite triangular array (n,k), $0 \le n < \infty$, $0 \le k \le n$ such that $(n,0) = (n,n) = 1$ and

$$(n+1, k+1) = (n,k) + (n,k+1). \tag{2.8}$$

When p is a prime, one can similarly obtain all *modular binomial coefficients* $(n,k)_p = \binom{n}{k} \pmod p$. The resulting modular Pascal triangle is self-similar in the following way (cf. Figure 2.1):

Let $0 < k < p$. Since p does not divide $(p-k)!k!$, we have $(p,k)_p = 0$. By (2.8), the triangular region $(p+n,k)_p$ with $0 \le n < p$, $0 < k < p$ contains only zeros. Using the same equation, when $1 < a < p$, the only nonzero entries in the anth row correspond to the entries of the apth row. Hence the first p^2 rows of the triangle can be tiled with triangles that contain either all zeros, or are suitable multiples of the first p rows.

The same self-similarity emerges for the p^s to p^{s+1} level of the modular Pascal triangle. There is therefore an easy way of calculating all modular binomial coefficients:

Theorem 2.11 (Lucas Theorem) *Let* p *be a prime,* $n = \sum_{i=0}^{s} n_i p^i$*,* $k = \sum_{i=0}^{s} k_i p^i$*, where* $0 \le k_i$*,* $n_i < p$*, for* $0 \le i \le s$*. Then*

$$\binom{n}{k} \equiv \prod_{i=0}^{s} \binom{n_i}{k_i} \pmod p,$$

where we set $\binom{a}{b} = 0$ *whenever* $a < b$*.*

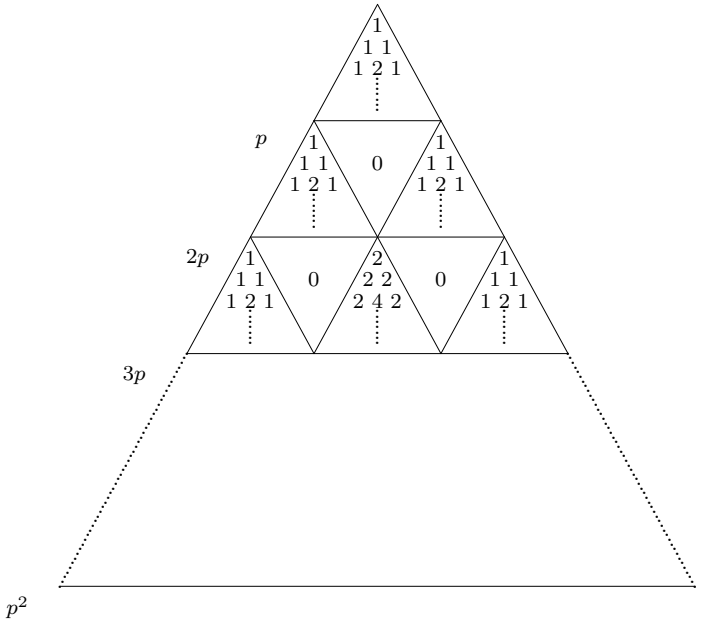

Figure 2.1: Modular Pascal triangle

Proof. Cut the first p^{s+1} rows of the modular Pascal triangle T by the p rows ap^s, $0 \le a < p$, and by the p antidiagonals bp^s, $0 \le b < p$. Label the resulting regions by (a, b). Then the intersection of the nth row and the kth antidiagonal will be in the region labelled (n_s, k_s), which consists of a triangular region that is an m multiple of the first p^s rows of T, and of an upside-down zero triangle. By the self-similarity, $m = \binom{n_s}{k_s}$, and the result follows by induction on s. □

Remark 2.12 Nearly all textbooks on number theory contain a short, elegant proof of Lucas Theorem. We opted for a longer but more intuitive proof. One of the first discussions concerning Lucas Theorem is [26].

Lemma 2.13 *Let p be a prime and a a nonnegative integer. Then the longest chain $a = a_0 > a_1 > \cdots > a_m$ such that $\binom{a_{i+1}}{a_i} \not\equiv 0 \pmod p$ has length $w_p(a)$.*

Proof. Let ℓ be the length of the longest regular chain for a. Theorem 2.11 shows that $\binom{m}{k} \not\equiv 0 \pmod p$ if and only if $m_i \ge k_i$ for every i (as both m_i, k_i are less than p and $\binom{m_i}{k_i}$ with $m_i \ge k_i$ is therefore not divisible by p). This means that $w_p(m) \ge w_p(k)$ must be satisfied whenever $\binom{m}{k} \not\equiv 0 \pmod p$, and $\ell \le w_p(a)$ follows.

On the other hand, if k is such that $k_i = m_i$ for each $i \ne j$, and $k_j = m_j - 1 \ge 0$, then $\binom{m}{k} \not\equiv 0 \pmod p$, by Theorem 2.11. Hence $\ell \ge w_p(a)$. □

We are ready to state the main result of this section:

Theorem 2.14 *Let F be a finite field of characteristic p, let V be an n-dimensional vector space over V, and let $f : V \longrightarrow F$ be a map. Then $f : V \longrightarrow F$ can be written as a reduced polynomial $f(\mathbf{x}) = \sum_{\mathbf{a} \in M(f)} \mathbf{x}^{\mathbf{a}}$ in $F[\mathbf{x}]$, where $\mathbf{x} = (x_1, \ldots, x_n)$, $\mathbf{a} = (a_1, \ldots, a_n)$, and $M(f)$ is the set of all multiexponents of f. Moreover,*

$$\operatorname{cdeg} f = \begin{cases} \infty, & \text{if } f(0) \neq 0, \\ \deg_p f, & \text{otherwise,} \end{cases}$$

where the p-degree $\deg_p f$ of f is calculated as

$$\deg_p f = \max_{(a_1,\ldots,a_n) \in M(f)} \sum_{i=1}^{n} w_p(a_i),$$

and where the p-weight $w_p(a_i)$ of $a_i = \sum_{j=0}^{q-1} a_{ij} p^j$, $0 \leq a_{ij} < p$, is the integer

$$w_p(a_i) = \sum_{j=0}^{q-1} a_{ij}.$$

Example 2.15 Let us illustrate with one simple example that the combinatorial degree is not so easy to calculate without Theorem 2.14. Let $f(x_1, x_2) = x_1^2 x_2$ over $GF(3) = \{0, 1, -1\}$. Then

$$\begin{aligned} \delta_2 f(\mathbf{x}, \mathbf{y}) &= (x_1 + y_1)^2 (x_2 + y_2) - x_1^2 x_2 - y_1^2 y_2 \\ &= (x_1^2 - x_1 y_1 + y_1^2)(x_2 + y_2) - x_1^2 x_2 - y_1^2 y_2 \\ &= x_1^2 y_2 - x_1 y_1 x_2 - x_1 y_1 y_2 + y_1^2 x_2, \end{aligned}$$

and thus

$$\begin{aligned} \delta_3 f(\mathbf{x}, \mathbf{y}, \mathbf{z}) &= (x_1 + y_1)^2 z_2 - (x_1 + y_1) z_1 (x_2 + y_2) - (x_1 + y_1) z_1 z_2 + z_1^2 (x_2 + y_2) \\ &\quad - x_1^2 z_2 + x_1 z_1 x_2 + x_1 z_1 z_2 - z_1^2 x_2 - y_1^2 z_2 + y_1 z_1 y_2 + y_1 z_1 z_2 - z_1^2 y_2 \\ &= - x_1 y_1 z_2 - x_1 y_2 z_1 - y_1 z_1 x_2 = -x_1 y_1 z_2 - x_1 y_2 z_1 - x_2 y_1 z_1, \end{aligned}$$

so that, finally,

$$\begin{aligned} \delta_4 f(\mathbf{x}, \mathbf{y}, \mathbf{z}, \mathbf{w}) &= - (x_1 + y_1) z_1 w_2 - (x_1 + y_1) z_2 w_1 - (x_2 + y_2) z_1 w_1 \\ &\quad + x_1 z_1 w_2 + x_1 z_2 w_1 + x_2 z_1 w_1 + y_1 z_1 w_2 + y_1 z_2 w_1 + y_2 z_1 w_1 \\ &= 0. \end{aligned}$$

Therefore $\operatorname{cdeg} f = 3$, as expected.

Remark 2.16 Combinatorial polarization was first studied by H. N. Ward. In [62], he proved that the combinatorial degree of a polynomial map over fields of characteristic 0 and over prime fields is equal to its degree. On pages 195–196 of [62], he claims that "It is not difficult to show that the combinatorial degree of a nonzero

polynomial over $GF(p^r)$ is the largest value of the sum of the p-weights of the exponents for the monomials appearing in the polynomial." This is exactly the statement of Theorem 2.14. To the author's knowledge, this is the first time the proof appeared in print.

Aschbacher [2] coined the name *derived forms* while working with combinatorial polarization in characteristic 2.

2.3 Graded subspaces of derived forms

As before, let V be an n-dimensional vector space over $F = GF(q)$, where $q = p^r$. Denote by $\Delta = \Delta(n, q)$ the vector space of all maps $f : V \longrightarrow F$, and let Δ_d be the subspace of Δ consisting of all maps $f : V \longrightarrow F$ with $\operatorname{cdeg} f \leq d$, where we allow $d = \infty$. Clearly $\Delta_{d_1} \subseteq \Delta_{d_2}$ if $d_1 \leq d_2$.

The dimension of $\Delta = \Delta_\infty$ is q^n, since this is the number or reduced monomials with coefficient 1. The purpose of this section is to use Theorem 2.14 in order to determine the dimensions of all subspaces Δ_d.

The only map in Δ_0 is the zero map, so $\dim \Delta_0 = 0$. In general, if B is a basis of Δ_{d-1}, it can be completed into a basis of Δ_d by adding all reduced monomials $f(\mathbf{x}) = \mathbf{x}^{\mathbf{a}}$ satisfying $\operatorname{cdeg} f = d$. This follows from Theorem 2.14 and Lemma 2.3.

Since $\operatorname{cdeg} \mathbf{x}^{\mathbf{a}} = \sum_{i=1}^{n} w_p(a_i)$, where $\mathbf{a} = (a_1, \ldots, a_n)$, and since $w_p(a_i)$ is equal to $\sum_{j=0}^{r-1} a_{ij}$, where $a_i = \sum_{j=0}^{r-1} a_{ij} p^j$, we will have to deal with ordered partitions of integers into sums of nonnegative integers.

Recall that the number of solutions to the equation

$$x_1 + \cdots + x_k = n \tag{2.9}$$

in nonnegative integers $x_1, \ldots, x_k$ is $\binom{n+k-1}{k-1}$ (cf. [51, Ch. 13]). Obviously, the solutions correspond to ordered partitions of the integer n into k nonnegative integers x_i.

In our situation, we have to consider restrictions on the size of the summands x_i. Let us therefore define the number $A(n, k, d)$ as the number of solutions to the equation (2.9), where we assume that every x_i is an integer satisfying $0 \leq x_i \leq d$. We immediately obtain:

Lemma 2.17 *$A(n, k, d) > 0$ if and only if $n \leq kd$. If $A(n, 1, d) > 0$, it is equal to 1. We have $A(n, k, d) = \binom{n+k-1}{k-1}$ for every $d \geq n$. The value $A(n, k, d)$ can be calculated recursively by*

$$A(n, k, d) = \sum_{i=0}^{d} A(n - i, k - 1, d). \tag{2.10}$$

Proof. Only (2.10) deserves proof. If $x_1 + \cdots + x_k = n$ and $x_1 = i$, we must have $x_2 + \cdots + x_k = n - i$. □

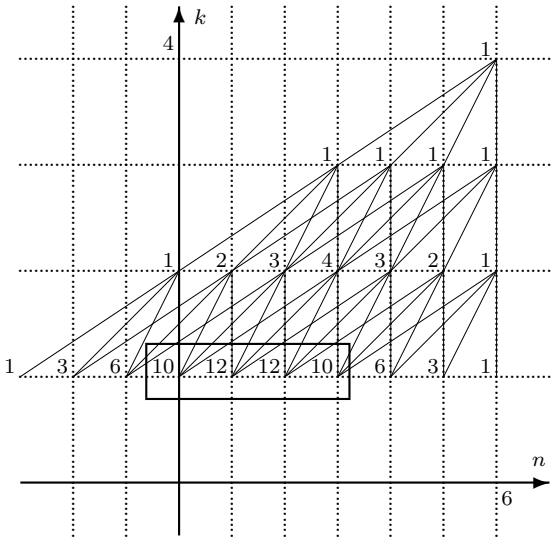

Figure 2.2: Calculating $A(6, 4, 3)$

Example 2.18 By (2.10), $A(5, 2, 3) = A(5, 1, 3)+A(4, 1, 3)+A(3, 1, 3)+A(2, 1, 3) = 0 + 0 + 1 + 1 = 2$. The two ordered partitions are $5 = 2 + 3 = 3 + 2$.

The recursive relation (2.10) can be nicely visualized (cf. Figure 2.2). To calculate $A(n, k, d)$, draw a point in the xy-plane with coordinates (n, k). Once a point (x, y) is placed, draw $d + 1$ edges connecting (x, y) with the points $(x - i, y - 1)$, where $0 \leq i \leq d$. Repeat until you reach the level $y = 1$. Then assign values to all drawn points as follows: Assign 1 to (n, k). Assume that (x, y) is a point such that the edges leading to (x, y) from above connect it with the points $(x, y+1), \ldots, (x+t, y+1)$, for some t. Then (x, y) is assigned the sum of the values at $(x, y + 1), \ldots, (x + t, y + 1)$. After all points have been assigned value, identify the values corresponding to the points $(0, 1), \ldots, (d, 1)$ (framed in Figure 2.2). Their sum is $A(n, k, d)$. For instance, we see in Figure 2.2 that $A(6, 4, 3) = 44$. The correctness of this procedure follows from Lemma 2.17.

The recursion in (2.10) can be avoided sometimes.

Lemma 2.19 *If $d \geq n/2$ then*

$$A(n, k, d) = \binom{n + k - 1}{k - 1} - \sum_{m=d+1}^{n} k \binom{n - m + k - 2}{k - 2}. \tag{2.11}$$

Proof. Let $x_1 + \cdots + x_k = n$ be a partition of n such that $0 \leq x_i$, for $1 \leq i \leq k$. If there is i such that $x_i > d$ then there is exactly one such i, as $n \leq 2d$. Upon removing this x_i, we obtain a partition $y_1 + \cdots + y_{k-1} = n - x_i$ such that $0 \leq y_j \leq d$.

Since $n - x_i \leq n - d \leq d$, the number of such partitions is the same as the number of partitions $z_1 + \cdots + z_{k-1} = n - x_i$ with $0 \leq z_j$. $\square$

Remark 2.20 In accordance with Figure 2.2, Lemma 2.19 yields

$$A(6,4,3) = \binom{9}{3} - 4\binom{4}{2} - 4\binom{3}{2} - 4\binom{2}{2} = 44.$$

Lemma 2.19 can be expanded by carefully analyzing the situation when d belongs to the interval $(\frac{n}{r+1}, \frac{n}{r}]$.

Proposition 2.21 *Let V be an n-dimensional vector space over the field $F = GF(q)$, where $q = p^r$. Let Δ_d be the vector space consisting of all maps $f : V \longrightarrow F$ with* $\operatorname{cdeg} f \leq d$. *Then* $\dim \Delta_0 = 0$, $\dim \Delta_\infty = q^n$ *and*

$$\dim \Delta_d = \sum_{t=1}^{d} \sum_{0 \leq w_i \leq r(p-1), \sum_{i=1}^{n} w_i = t} \prod_{j=1}^{n} A(w_i, r, p-1) \tag{2.12}$$

for $0 < d < \infty$.

Proof. Assume that $0 \leq d < \infty$. Let us count the number of reduced monomials $f(\mathbf{x}) = \mathbf{x}^{\mathbf{a}}$ with $\operatorname{cdeg} f = t$, where $\mathbf{a} = (a_1, \ldots, a_n)$, and $a_i = \sum_{j=0}^{r} a_{ij} p^j$, $0 \leq a_{ij} < p$.

Assume that the p-weights $w_i = w_p(a_i)$ are fixed. Then there are exactly $A(w_i, r, p-1)$ ways in which the coefficients a_{ij} of the p-ary expansion of a_i can be chosen so that $w_i = \sum_{j=0}^{r} a_{ij}$.

The second sum of (2.12) accounts for all possible ways in which $\operatorname{cdeg} f = \sum_{i=1}^{n} w_i$ can be equal to t. The first sum of (2.12) then accounts for all reduced monomials with $\operatorname{cdeg} f = t \leq d$. $\square$

Admittedly, Proposition 2.21 is not practical, since we must not only calculate several values $A(n, k, d)$, but also exhibit all partitions of all integers $1 \leq t \leq d$ into sums of nonnegative integers $w_1, \ldots, w_n$. The case $q = 2$ can be greatly simplified, since any nonzero exponent is necessarily equal to 1, and hence the combinatorial degree of a reduced monomial f is just the number of nonzero exponents of f.

Corollary 2.22 *Assume that V, F and Δ_d are as in Proposition* 2.21*, with $q = p = 2$, $1 \leq d < \infty$. Then* $\dim \Delta_d = \sum_{1 \leq t \leq d} \binom{n}{t}$.

2.4 Factor sets

Before we turn our attention to the connections between derived forms, code loops and high-level codes, we must introduce factor sets.

Let Q be a loop and A an abelian group, with multiplication written additively. Let $\varphi : Q \longrightarrow \operatorname{Aut}(A)$ be a homomorphism, and let $\eta : Q \times Q \longrightarrow A$ be an arbitrary map. Define new multiplication on $Q \times A$ by

$$(x, a)(y, b) = (xy, a^{\varphi(y)} + b + \eta(x, y)), \tag{2.13}$$

where $a^{\varphi(y)}$ stand for the image of a under $\varphi(y) \in \mathrm{Aut}(A)$. The resulting groupoid will be denoted by $E = (Q, A, \varphi, \eta)$.

Lemma 2.23 *Lat Q be a loop, A an abelian group, $\varphi : Q \longrightarrow \mathrm{Aut}(A)$ a homomorphism and $\eta : Q \times Q \longrightarrow A$ a map. Then $E = (Q, A, \varphi, \eta)$ is a quasigroup. It is a loop if and only if there is $c \in A$ such that*

$$\eta(x, 1) = c, \quad \eta(1, x) = c^{\varphi(x)} \tag{2.14}$$

holds for every $x \in Q$. The neutral element of E is then $(1, -c)$.

Proof. Given (x, a), (z, c), we must show that there is a unique (y, b) such that $(x, a)(y, b) = (z, c)$. By (2.13), we must have $y = x^{-1}z$. Then $c = a^{\varphi(x^{-1}z)} + b + \eta(x, x^{-1}z)$, and b is uniquely determined by (x, a), (z, c), too. Similarly when (y, b) and (z, c) are given. Thus E is a quasigroup.

Assume there is $c \in A$ such that (2.14) holds for every $x \in Q$. Then

$$\begin{aligned} (1, -c)(y, b) &= (y, -c^{\varphi(y)} + b + \eta(1, y)) = (y, b), \\ (x, a)(1, -c) &= (x, a^{\varphi(x)} - c + \eta(x, 1)) = (x, a) \end{aligned}$$

for every (x, a), (y, b). Hence E is a loop with neutral element $(1, -c)$.

Conversely, assume that E is a loop with neutral element $(z, -c)$, for some $z \in Q$, $c \in A$. Since $(x, a) = (x, a)(z, -c) = (xz, a^{\varphi(x)} - c + \eta(x, z))$, we must have $z = 1$. Then $a = a - c + \eta(x, 1)$, and $c = \eta(x, 1)$ follows. Moreover, $(y, b) = (1, -c)(y, b) = (y, -c^{\varphi(y)} + b + \eta(1, y))$ implies $\eta(1, y) = c^{\varphi(y)}$. $\square$

We will assume from now on that E is a loop and $c = 0$. Every pair (φ, η) satisfying (2.14) with $c = 0$ is called a *factor set*. We have $A \cong (1, A) \leq E$, as $(1, a)(1, b) = (1, a + b)$. Moreover, when we define an equivalence $\sim$ on $Q \times A$ by $(x, a) \sim (x, b)$, we see that $E/\sim$ is isomorphic to Q. It then comes as no surprise when we call E an *extension of A by Q*.

Lemma 2.24 *Assume that $E = (Q, A, \varphi, \eta)$ is a loop. Then E is Moufang if and only if Q is Moufang and*

$$\eta(x, y)^{\varphi(xz)} + \eta(xy, x)^{\varphi(z)} + \eta(xy \cdot x, z) = \eta(x, z) + \eta(y, xz) + \eta(x, y \cdot xz) \tag{2.15}$$

holds for every x, y, $z \in Q$.

Proof. Recall the Moufang identity $((xy)x)z = x(y(xz))$. Direct calculation yields

$$\begin{aligned} &(((x, a)(y, b))(x, a))(z, c) \\ &= ((xy,\ a^{\varphi(y)} + b + \eta(x, y))(x, a))(z, c) \\ &= ((xy)z,\ a^{\varphi(yx)} + b^{\varphi(x)} + \eta(x, y)^{\varphi(x)} + a + \eta(xy, x))(z, c) \\ &= (((xy)x)z,\ a^{\varphi((yx)z)} + b^{\varphi(xz)} + a^{\varphi(z)} + \eta(xy, x)^{\varphi(z)} + c + \eta((xy)x, z)), \end{aligned}$$

and similarly

$$\begin{aligned}
&(x,a)((y,b)((x,a)(z,c)))\\
&= (x,a)((y,b)(xz,\ a^{\varphi(z)} + c + \eta(x,z)))\\
&= (x,a)(y(xz),\ b^{\varphi(xz)} + a^{\varphi(z)} + c + \eta(x,z) + \eta(y,xz))\\
&= (x(y(xz)),\ a^{\varphi(y(xz))} + b^{\varphi(xz)} + a^{\varphi(z)} + c + \eta(x,z) + \eta(y,xz) + \eta(x,y(xz))).
\end{aligned}$$

The first components coincide if and only if Q is Moufang. Since φ is a homomorphism, the second components coincide if and only if (2.15) holds. □

Every factor set (φ, η) satisfying (2.15) is called a *Moufang factor set*.

Remark 2.25 Is is not hard to show that E is associative (hence a group) if and only if Q is a group and

$$\eta(x,y)^{\varphi(z)} + \eta(xy,z) = \eta(y,z) + \eta(x,yz)$$

holds for every x, y, $z \in Q$.

2.5 Code loops and doubly even codes

In this section, let $F = \{0,1\}$ be the two-element field and V a finite-dimensional vector space over F.

In the context of coding theory, every subspace C of V is called a (*binary linear*) *code*, and every element $c \in C$ is a *codeword*. We will assume that a basis of V is fixed. Then the *Hamming weight* $w(c)$ is the number of nonzero coordinates of c. The dimension of V is called the *length* of C.

A code $C \leq V$ is of *level* r if 2^r divides $w(c)$ for every $c \in C$, and if r is as big as possible. When $r = 2$, we speak of *doubly even codes*.

Many good codes are doubly even. For instance, the extended binary Golay code (of length 24 and dimension 12) consists of certain codewords of Hamming weight 0, 8, 12, 16 and 24 (cf. [50]), and is therefore doubly even.

Consider any *Hamming code* C of length $2^r - 1$, i.e., a code whose parity-check matrix H consists of all $2^r - 1$ nonzero vectors of length r. Then H^T generates a code D of dimension r—the *dual* of C. Clearly, every basis vector d of D satisfies $w(d) = 2^{r-1}$. It is not hard to show that the same holds for any nonzero $d \in D$. In particular, D is of level $r - 1$. We will use this fact in Theorem 2.31.

Given two vectors u, $v \in V$, denote by $u \cap v$ the vector whose ith coordinate is equal to 1 if and only if the ith coordinates of both u and v are equal to 1. Using a double counting argument, we obtain

$$w(u) + w(v) = w(u+v) + 2w(u \cap v) \tag{2.16}$$

for any u, $v \in V$, cf. Figure 2.3. This simple observation allows us to enter combinatorial polarization into play.

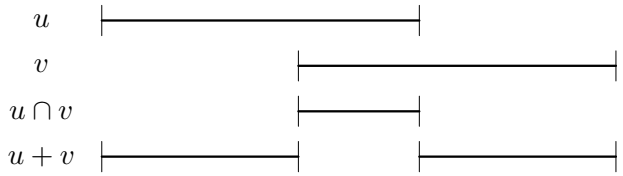

Figure 2.3: Hamming weights over $GF(2)$

Lemma 2.26 *Let V be a finite-dimensional vector space over F. Then the Hamming weight $w : V \longrightarrow \mathbb{N}$ satisfies*

$$\delta_m w(u_1, \ldots, u_m) = 2^{m-1} w(u_1 \cap \cdots \cap u_m)$$

for every $m \geq 1$.

Proof. We use induction on m. When $m = 1$, there is nothing to prove as $\delta_1 w = w$. Assume the lemma holds for m, and pick $u_1, \ldots, u_{m+1} \in V$. Then

$$\begin{aligned}
&\delta_{m+1} w(u_1, \ldots, u_{m+1}) \\
&= \delta_m w(u_1 + u_2, u_3, \ldots, u_{m+1}) - \delta_m w(u_1, u_3, \ldots, u_{m+1}) - \delta_m w(u_2, u_3, \ldots, u_{m+1}) \\
&\qquad = 2^{m-1} \Big(w((u_1 + u_2) \cap c) - w(u_1 \cap c) - w(u_2 \cap c) \Big),
\end{aligned}$$

where $c = u_3 \cap \cdots \cap u_{m+1}$. With $u = u_1 \cap c$, $v = u_2 \cap c$, we have $u + v = (u_1 + u_2) \cap c$ and $u \cap v = u_1 \cap u_2 \cap c$. By (2.16),

$$w((u_1 + u_2) \cap c) - w(u_1 \cap c) - w(u_2 \cap c) = 2w(u_1 \cap u_2 \cap c),$$

and we are through. □

Code loops were originally defined by Griess [32] as follows: Let C be a doubly even code over $F = \{0, 1\}$. Let $\eta : C \times C \longrightarrow F$ be a map satisfying

$$\eta(x, x) = w(x)/4, \tag{2.17}$$
$$\eta(x, y) + \eta(y, x) = w(x \cap y)/2, \tag{2.18}$$
$$\eta(x, y) + \eta(x + y, z) + \eta(y, z) + \eta(x, y + z) = w(x \cap y \cap z), \tag{2.19}$$

for x, y, $z \in C$. Then $C \times F$ with multiplication

$$(x, a)(y, b) = (x + y, a + b + \eta(x, y)) \tag{2.20}$$

is a *code loop*.

Construction (2.20) is a special case of (2.13) with trivial homomorphism $\varphi : C \longrightarrow \mathrm{Aut}(F)$. Substituting $x = 0$, $y = z$ into (2.19) yields $\eta(0, y) = 0$, and then

(2.18) implies $\eta(y,0) = 0$, too. Hence a code loop is indeed a loop, by Lemma 2.23. Griess shows in [32] that, up to equivalence, there is a unique code loop for every doubly even code C. He also shows that every code loop is Moufang, and we will give a proof similar to his. First, we need a simple lemma about combinatorial polarization over $\{0,1\}$.

Lemma 2.27 *Let $f : V \longrightarrow F = \{0,1\}$ be a map satisfying $f(0) = 0$. Then $\delta_s f(v_1, v_2, \ldots, v_s) = 0$ whenever $v_1 = 0$ or $v_1 = v_2$.*

Proof. The polarization identity (2.2) with $v_1 = 0$ yields

$$\delta_s f(v_1, \ldots, v_s) = \delta_{s-1} f(0, v_3, \ldots, v_s) + \delta_{s-1} f(v_2, \ldots, v_s) + \delta_{s-1} f(0 + v_2, v_3, \ldots, v_s),$$

which equals 0 by induction on s. Then $\delta_s f(v_1, v_1, v_3, \ldots, v_s) = \delta_s f(v_1, v_3, \ldots, v_s) + \delta_s f(v_1, v_3, \ldots, v_s) + \delta_s f(v_1 + v_1, v_3, \ldots, v_s) = 0$. □

In fact, $\delta_s f(v_1, \ldots, v_s)$ over $\{0,1\}$ vanishes anytime the vectors v_1, …, v_s are linearly dependant. We will not need this fact below.

Lemma 2.28 *Every code loop is Moufang.*

Proof. We must show that (2.15) holds, i.e., that

$$\eta(x,y) + \eta(x+y,x) + \eta(y,z) + \eta(x,z) + \eta(y,x+z) + \eta(x,y+x+z) = 0 \quad (2.21)$$

holds for every x, y, $z \in C$. Condition (2.19) with $x + z$ in place of z yields

$$\eta(x,y) + \eta(x+y,x+z) + \eta(y,x+z) + \eta(x,y+x+z) + w(x \cap y \cap z) = 0,$$

because $w(x \cap y \cap z) = w(x \cap y \cap (x+z))$, by Lemmas 2.26 and 2.27. Hence (2.21) holds if and only if

$$\eta(x+y,x) + \eta(y,z) + \eta(x,z) + \eta(x+y,x+z) + w(x \cap y \cap z) = 0.$$

The last equation follows from (2.19) with $x + y$ in place of x, again using the fact that $w(x \cap y \cap z) = w((x+y) \cap y \cap z)$. □

Chein and Goodaire found a nice characterization of code loops. Namely, they show (cf. [12, Thm. 5]) that code loops are exactly finite Moufang loops with at most two squares. Their proof is based on three observations:

First, if L is a Moufang loop with $|L^2| \leq 2$ then every commutator and associator belongs to L^2 and

$$\begin{aligned} (xy)^2 &= x^2 y^2 [x,y], \\ [xy,z] &= [x,z][y,z][x,y,z], \\ [vx,y,z] &= [v,y,z][x,y,z] \end{aligned} \quad (2.22)$$

holds for every v, x, y, $z \in L$ (see [12, Thm. 1, 2]). In other words, if we set $Z = L^2$ then L/Z is an elementary abelian 2-group, and the well-defined map $P : L/Z \longrightarrow Z$, $x \mapsto x^2$ satisfies $\delta_2 P(x, y) = [x, y]$, $\delta_3 P(x, y, z) = [x, y, z]$, $\operatorname{cdeg} P = 3$, as can be seen immediately from (2.2) and (2.22). Note that under these circumstances L is an elementary abelian 2-group if and only if $|L^2| = 1$.

Second, if $L = C \times F$ is a code loop for C and $x = (\tilde{x}, a)$, $y = (\tilde{y}, b)$, $z = (\tilde{z}, c)$ belong to L then

$$\begin{aligned} x^2 &= (0, w(\tilde{x})/4), \\ [x, y] &= (0, w(\tilde{x} \cap \tilde{y})/2), \\ [x, y, z] &= (0, w(\tilde{x} \cap \tilde{y} \cap \tilde{z})), \end{aligned} \tag{2.23}$$

by [12, Lm. 6]. (This implies (2.22), by Lemma 2.26.)

Third, given an integer $n \geq 1$ and parameters α_i, β_{ij}, $\gamma_{ijk} \in \{0, 1\}$, for $1 \leq i$, j, $k \leq n$, there is a doubly even code C with basis $c_1, \ldots, c_n$ such that

$$\begin{aligned} \alpha_i &= w(c_i), \\ \beta_{ij} &= w(c_i \cap c_j), \\ \gamma_{ijk} &= w(c_i \cap c_j \cap c_k), \end{aligned} \tag{2.24}$$

for $1 \leq i$, j, $k \leq n$ (cf. the proof of [12, Thm. 5]). It is this construction that turns out to be the most difficult part of the proof that code loops are exactly finite Moufang loops with at most two squares. We simplify and generalize the construction in the next section. The construction presented below is easier than that of [52], too, because it avoids induction.

To conclude our discussion concerning code loops, note that a map $f : V \longrightarrow \{0, 1\}$ with combinatorial degree 3 is uniquely specified if we know the values of $f(e_i)$, $f(e_i + e_j)$ and $f(e_i + e_j + e_k)$ for some basis $e_1, \ldots, e_n$ of V. Hence, by (2.22), (2.23) and (2.24), code loops can be identified with maps $P : V \longrightarrow \{0, 1\}$ of combinatorial degree 3.

Remark 2.29 See [35] for a discussion concerning code loops, symplectic cubic spaces and small Frattini Moufang loops, [36] for an explicit construction of the Parker loop, i.e., the code loop of the extended binary Golay code, and [46] for a generalization of code loops into odd characteristic.

2.6 High-level binary codes

In this section, we present a generalization of the above-mentioned result of Chein and Goodaire.

Let V be an m-dimensional vector space over $F = \{0, 1\}$, and let $P : V \longrightarrow F$ be a map satisfying $P(0) = 0$. Then P can be identified with some polynomial in $F[x_1, \ldots, x_m]$, as we have argued in Section 2.2. As in (2.4), we can write P as

$$P(x_1, \ldots, x_m) = \sum_{J \in \mathcal{J}} \prod_{j \in J} x_j,$$

where the summation runs over some set $\mathcal{J}$ of subsets of $\{1, \ldots, m\}$.

Lemma 2.30 *Calculating in $F[x_1, \ldots, x_m]$, we have*

$$\prod_{i\in\{1,\ldots,m\}} x_i = \sum_{J\in\mathcal{J}} \Big(1 + \prod_{j\in J}(1 + x_j)\Big),$$

for some set of subsets $\mathcal{J}$.

Proof. We prove the lemma by induction on m. When $m = 1$, we have $x_1 = 1 + (1 + x_1)$. Assume that the lemma holds for m. We have

$$\prod_{i\in\{1,\ldots,m+1\}} (1 + x_i) = \sum_{J\subseteq\{1,\ldots,m+1\}} \prod_{j\in J} x_j,$$

and hence

$$\prod_{i\in\{1,\ldots,m+1\}} x_i = \Big(1 + \prod_{i\in\{1,\ldots,m+1\}} (1 + x_i)\Big) + \sum_{J} \prod_{j\in J} x_j,$$

where each subset J has at most m elements. We are done by the induction hypothesis. □

Therefore, every map $P : V \longrightarrow F$ can be written as

$$P(x_1, \ldots, x_m) = \sum_{J\in\mathcal{J}} \Big(1 + \prod_{j\in J} x'_j\Big), \tag{2.25}$$

where the summation runs over some set $\mathcal{J}$ of subsets $\{1, \ldots, m\}$, and where $x'_j \equiv x_j + 1 \pmod 2$.

Theorem 2.31 *Let V be an m-dimensional vector space over $F = \{0, 1\}$, and let $P : V \longrightarrow F$ be such that $P(0) = 0$ and $\operatorname{cdeg} P = r + 1$. Then there is a binary linear code C isomorphic to V and of level r such that $w(c)/2^r \equiv P(c) \pmod 2$ for every $c \in C$.*

Proof. Identify $P : V \longrightarrow F$ with a polynomial

$$P(x_1, \ldots, x_m) = \sum_{J\in\mathcal{J}} \Big(1 + \prod_{j\in J} x'_j\Big), \tag{2.26}$$

as in (2.25). By Theorem 2.14, $r + 1 = \operatorname{cdeg} P = \deg_2 P \le m$. Now, $\deg_2 f = \deg f$.

Let H be the parity-check matrix of the Hamming code of dimension $r + 1$ (and length $2^{r+1} - 1$). Hence the rows of H are exactly the nonzero vectors of F^{r+1}, in some order. Let D be the code whose generating matrix is the transpose of H. As we have already remarked in Section 2.5, $w(d) = 2^r$ for every nonzero $d \in D$. Every

codeword d can be written as a linear combination of the columns of H, and hence identified with some $(d_1, \ldots, d_{r+1}) \in F^{r+1}$. Note that

$$w(d)/2^r \equiv 1 + \prod_{i=1}^{r+1} d'_i, \tag{2.27}$$

since the product $\prod_{i=1}^{r+1} d'_i$ vanishes for every nonzero $d \in D$.

For every subset $J = \{j_1, \ldots, j_t\}$ in $\mathcal{J}$ define the map $\pi_J : V \longrightarrow D$ by

$$\pi_J(x_1, \ldots, x_m) = (x_{j_1}, \ldots, x_{j_t}, 0, \ldots, 0) \in F^{r+1}.$$

This map is well-defined because $\deg P \leq m$. For $x \in V$, let $\pi(x) = \bigoplus_{J \in \mathcal{J}} \pi_J(x)$, and let C be the image of V under π. Then C is isomorphic to V, and, for $x = (x_1, \ldots, x_m) \in V$,

$$P(x) \overset{(2.26)}{=} \sum_{J \in \mathcal{J}} \Big(1 + \prod_{j \in J} x'_j\Big) \overset{(2.27)}{\equiv} \sum_{J \in \mathcal{J}} w(\pi_J(x))/2^r = w(\pi(x))/2^r.$$

This finishes the proof. □

Example 2.32 We will work out an example illustrating the proof of Theorem 2.31. Let $P : V = F^3 \longrightarrow F$ be the map $P(x_1, x_2, x_3) = x_2 + x_1x_3 + x_1x_2x_3$. Then

$$P(x_1, x_2, x_3) = (1 + x'_1x'_2) + (1 + x'_2x'_3) + (1 + x'_1x'_2x'_3),$$

so that $\mathcal{J} = \{\{1, 2\}, \{2, 3\}, \{1, 2, 3\}\}$. We have $\operatorname{cdeg} P = \deg P = 3 = r + 1$, and $m = \dim V = 3$.

The construction depends on a choice of the (dual) Hamming code. Let us pick the code whose generating matrix is

$$H^T = \begin{pmatrix} 1000111 \\ 0101011 \\ 0011101 \end{pmatrix}.$$

The explicit construction also depends on an ordering of the elements of $\mathcal{J}$. Let us agree that they are ordered as above.

Let $e_1 = (1, 0, 0)$, $e_2 = (0, 1, 0)$, $e_3 = (0, 0, 1)$ be the canonical basis for V. Then, with respect to the basis consisting of the three rows of H^T, the vectors e_1, e_2, e_3 are mapped onto

$$\begin{aligned} \pi(e_1) &= (1, 0, 0) \oplus (0, 0, 0) \oplus (1, 0, 0) = c_1, \\ \pi(e_2) &= (0, 1, 0) \oplus (1, 0, 0) \oplus (0, 1, 0) = c_2, \\ \pi(e_3) &= (0, 0, 0) \oplus (0, 1, 0) \oplus (0, 0, 1) = c_3. \end{aligned}$$

For instance, the middle summand of c_3 is $(0, 1, 0)$ because $\pi_{\{2,3\}}(0, 0, 1) = (0, 1, 0)$.

Viewed as vectors over F, the vectors c_1, c_2, c_3 (forming a basis of C) become

$$\begin{aligned} c_1 &= (1000111, 0000000, 1000111), \\ c_2 &= (0101011, 1000111, 0101011), \\ c_3 &= (0000000, 0101011, 0011101). \end{aligned}$$

Let us test Theorem 2.31 on two vectors. First, let $x = e_2$. Then $P(x) = 1+0+0 = 1$, $c = \pi(x) = c_2$, and $w(c)/2^2 = 12/4 = 3$. Similarly, with $x = e_1 + e_2 + e_3$, we obtain $P(x) = 1 + 1 \cdot 1 + 1 \cdot 1 \cdot 1 = 3$,

$$c = \pi(x) = c_1 + c_2 + c_3 = (1101100, 1101100, 1110001),$$

and $w(c)/2^2 = 12/4 = 3$. In both cases, $w(c)/2^r \equiv P(x) \pmod 2$.

The construction of Theorem 2.31 allows us to calculate the length of the resulting code C over F:

Corollary 2.33 *Let P, C be as in Theorem* 2.31*,*

$$P(x_1, \ldots, x_m) = \sum_{J \in \mathcal{J}} \Big(1 + \prod_{j \in J} x'_j\Big).$$

Then the length of C over F is equal to $|\mathcal{J}| \cdot (2^{\deg P} - 1)$.

2.7 Codes, code loops and designs

An interesting phenomenon emerges when the details of the polynomial P for the extended binary Golay code $\mathcal{G}$ are calculated. We offer this section as a motivation for future research.

Let us go through the Mathematica [40] calculations first.

As in [34, p. 77], we use $G = (I_{12}|B)$ as the generating matrix for $\mathcal{G}$, where I_{12} is the 12×12 identity matrix and

$$B = \begin{pmatrix} 1 & 1 & 0 & 1 & 1 & 1 & 0 & 0 & 0 & 1 & 0 & 1 \\ 1 & 0 & 1 & 1 & 1 & 0 & 0 & 0 & 1 & 0 & 1 & 1 \\ 0 & 1 & 1 & 1 & 0 & 0 & 0 & 1 & 0 & 1 & 1 & 1 \\ 1 & 1 & 1 & 0 & 0 & 0 & 1 & 0 & 1 & 1 & 0 & 1 \\ 1 & 1 & 0 & 0 & 0 & 1 & 0 & 1 & 1 & 0 & 1 & 1 \\ 1 & 0 & 0 & 0 & 1 & 0 & 1 & 1 & 0 & 1 & 1 & 1 \\ 0 & 0 & 0 & 1 & 0 & 1 & 1 & 0 & 1 & 1 & 1 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 & 0 & 1 & 1 & 1 & 0 & 1 \\ 0 & 1 & 0 & 1 & 1 & 0 & 1 & 1 & 1 & 0 & 0 & 1 \\ 1 & 0 & 1 & 1 & 0 & 1 & 1 & 1 & 0 & 0 & 0 & 1 \\ 0 & 1 & 1 & 0 & 1 & 1 & 1 & 0 & 0 & 0 & 1 & 1 \\ 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 0 \end{pmatrix}.$$

Let $P : \mathcal{G} \longrightarrow F = \{0, 1\}$ be the map such that $P(c) = w(c)/4 \pmod 2$. Using the basis of $\mathcal{G}$ consisting of the rows of G, we can identify P with a polynomial in $F[x_1, \ldots, x_{12}]$. Here is $P(x_1, \ldots, x_{12})$ obtained by Mathematica upon simplifying the interpolation polynomial (2.3):

$$
\begin{aligned}
&x_1x_3x_4 + x_1x_4x_5 + x_2x_4x_5 + x_1x_2x_6 + x_1x_4x_6 + x_2x_5x_6 + x_3x_5x_6 + x_1x_3x_7 + \\
&x_2x_3x_7 + x_2x_5x_7 + x_3x_6x_7 + x_4x_6x_7 + x_2x_4x_8 + x_3x_4x_8 + x_1x_6x_8 + x_3x_6x_8 + \\
&x_1x_7x_8 + x_4x_7x_8 + x_5x_7x_8 + x_1x_2x_9 + x_1x_3x_9 + x_3x_5x_9 + x_4x_5x_9 + x_2x_7x_9 + \\
&x_4x_7x_9 + x_2x_8x_9 + x_5x_8x_9 + x_6x_8x_9 + x_1x_2x_{10} + x_2x_3x_{10} + x_2x_4x_{10} + \\
&x_1x_5x_{10} + x_4x_6x_{10} + x_5x_6x_{10} + x_1x_7x_{10} + x_3x_8x_{10} + x_5x_8x_{10} + x_3x_9x_{10} + \\
&x_6x_9x_{10} + x_7x_9x_{10} + x_2x_3x_{11} + x_3x_4x_{11} + x_1x_5x_{11} + x_3x_5x_{11} + x_2x_6x_{11} + \\
&x_5x_7x_{11} + x_6x_7x_{11} + x_1x_8x_{11} + x_2x_8x_{11} + x_1x_9x_{11} + x_4x_9x_{11} + x_6x_9x_{11} + \\
&x_4x_{10}x_{11} + x_7x_{10}x_{11} + x_8x_{10}x_{11} + \\
&x_{12} + \sum_{1 \le i \le 11} x_ix_{12} + \sum_{1 \le i < j \le 12} x_ix_jx_{12}.
\end{aligned}
$$

Now, let us consider all 55 monomials of $P(x_1, \ldots, x_{12})$ not involving the variable x_{12}. Let $\mathcal{P} = \{1, \ldots, 11\}$, and let $\mathcal{B}$ be a set of subsets of $\mathcal{P}$ such that $B = \{i, j, k\}$ belongs to $\mathcal{B}$ if and only if $x_ix_jx_k$ is a monomial of $P(x_1, \ldots, x_{12})$. (We have discarded all monomials involving the last variable x_{12} because we have started from the extended Golay code.)

Recall that, in general, an incidence relation $(\mathcal{P}, \mathcal{B})$ is called a t-(v, k, λ) *design* if $|\mathcal{P}| = v$, $|B| = k$ for every $B \in \mathcal{B}$, and any t distinct points of $\mathcal{P}$ form a subset of exactly λ blocks $B \in \mathcal{B}$.

One can then verify by hand that $(\mathcal{P}, \mathcal{B})$ constructed above is a 2-$(11, 3, 3)$ design, the only tedious part being the check that every one of the $\binom{11}{2} = 55$ subsets $\{i, j\}$ of $\mathcal{P}$ is contained in exactly three blocks of $\mathcal{B}$.

Forgetting about $\mathcal{G}$, we could now use P and Theorem 2.31 to construct a code isomorphic to $\mathcal{G}$ having the same intersecting properties as $\mathcal{G}$, whatever that means. Unfortunately, the resulting code would be very long compared to $\mathcal{G}$. (First, we would have to rewrite P as in the proof of Theorem 2.31, and then use Corollary 2.33 to find the length of the code.)

In any case, the fact that the 2-$(11, 3, 3)$ design appeared deserves some explanation. We could also proceed backwards: to start with any design, construct a polynomial, and then apply Theorem 2.31 to obtain a binary code with interesting intersecting properties. Nevertheless, in order to obtain practical (that is short) codes, a better construction than that of Theorem 2.31 is needed.

Chapter 3

Moufang Loops with a Subgroup of Index Two

Many Moufang loops are of the type $M(G,2)$, defined below. We will illustrate this fact in Section 3.2. Some recent results (cf. [24]) indicate that loops $M(G,2)$ can be used as building blocks of all Moufang 2-loops. This topic is discussed in detail in Chapter 5.

We prove in Section 3.1 that the construction $M(G,2)$ is unique, in a sense. In fact, we also show that no nonMoufang Bol loop can be obtained by any similar construction. (We will be more precise below.) Section 3.2 deals with presentations for loops $M(G,2)$ when G is 2-generated. Finally, Section 3.3 offers a neat visual description of the smallest nonassociative Moufang loop $M(S_3,2)$, where S_3 is the symmetric group on 3 points.

Section 3.1 is based on [59], Sections 3.2 and 3.3 on [61].

3.1 Loops M(G,2)

Chein introduced the following construction in [11] to obtain Moufang loops from groups: Let G be a finite group and let $\overline{G} = \{\overline{x};\ x \in G\}$ be a set of new elements. Define multiplication $*$ on $G \cup \overline{G}$ by

$$x * y = xy, \quad x * \overline{y} = \overline{yx}, \quad \overline{x} * y = \overline{xy^{-1}}, \quad \overline{x} * \overline{y} = y^{-1}x, \tag{3.1}$$

where x, $y \in G$. The resulting Moufang loop $M(G,2)$ is associative if and only if G is abelian, according to [11].

We are going to study a generalization of Chein's construction (3.1). Given a group G, consider the 8 multiplicative operations on G: $(x,y) \mapsto (x^i y^j)^k$, where i, j, $k \in \{-1,1\}$. Let C_2 be the cyclic group of order 2. Define a new multiplication on $G \times C_2$ by assigning one of the above 8 multiplications to each quarter $(G \times \{i\}) \times (G \times \{j\})$, for i, $j \in C_2$. Let M be the resulting groupoid.

It this section, we characterize when M is a loop (Lemma 3.1); we show that if M is a Bol loop, it is Moufang (Lemma 3.2); and we prove that for any group G there are

exactly 4 assignments that yield nonassociative Moufang loops, all (anti)isomorphic to the loop $M(G,2)$. See Theorem 3.6 for details.

Chein's construction (3.1) is therefore unique, in this sense.

3.1.1 Notation

Let us introduce a notation that will better serve our purposes. First of all, in this section we will write maps to the right of their arguments and compose them accordingly. Consider the permutations ι, σ, τ of $G \times G$ defined by $(x,y)\iota = (x,y)$, $(x,y)\sigma = (y,x)$, and $(x,y)\tau = (y^{-1},x)$. Since $\sigma^2 = \tau^4 = \iota$ and $\sigma\tau\sigma = \tau^{-1}$, the group A generated by σ and τ is isomorphic to Q_8, the quaternion group of order 8. The elements ψ of A are described by

ψ	ι	σ	τ	τ^2	τ^3	$\sigma\tau$	$\sigma\tau^2$	$\sigma\tau^3$
$(x,y)\psi$	(x,y)	(y,x)	(y^{-1},x)	(x^{-1},y^{-1})	(y,x^{-1})	(x^{-1},y)	(y^{-1},x^{-1})	(x,y^{-1}).

We like to think of these elements as multiplications in G, and often identify $\psi \in A$ with the map $\psi\Delta : G\times G \longrightarrow G$, where $(x,y)\Delta = xy$. For instance, the permutation $\sigma\tau$ determines the multiplication $x*y = x^{-1}y$. Note that $\sigma\Delta = \iota\Delta$ when G is abelian, and that $A\Delta = \iota\Delta$ when G is an elementary abelian 2-group.

To avoid trivialities, we assume throughout this section that *G is not an elementary abelian 2-group, and that $|G| > 1$.*

It is natural to split the multiplication table of $M(G,2)$ into four quarters $G\times G$, $G \times \overline{G}$, $\overline{G} \times G$ and $\overline{G} \times \overline{G}$, as in

$*$	G	$\overline{G}$
G		
$\overline{G}$		

.

Then Chein's construction (3.1) can be represented by the matrix

$$M_c = \begin{pmatrix} \iota & \sigma \\ \sigma\tau^3 & \tau \end{pmatrix}. \tag{3.2}$$

For example, we can see from M_c that $\overline{x} * y = \overline{(x,y)\sigma\tau^3} = \overline{xy^{-1}}$, for x, $y \in G$.

3.1.2 Uniqueness

Looking at Chein's construction 3.1) via (3.2), it appears to be somewhat arbitrary. Let us therefore investigate all multiplications

$$M = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix}, \tag{3.3}$$

where α, β, γ, $\delta \in A$. We will no more distinguish between the matrix M and the groupoid it defines.

We note in passing that every M is a quasigroup. The next lemma characterizes all loops M. In the course of the proof we encounter several identities of the form

$w_1 = w_2$, where w_i is a word in some symbols $x_1, \ldots, x_m \in G$. When w_1, w_2 reduce to the same word in the free group on $x_1, \ldots, x_m$, then $w_1 = w_2$ surely holds in G. Conversely, since we assumed that G is not an elementary abelian 2-group and $|G| > 1$, there are many identities that do not hold in G, no matter what G is. For instance, $x = x^{-1}$, $y = xy^{-1}x^{-1}$ (set $x = y$), and so on.

Lemma 3.1 *M is a loop if and only if $\alpha \in \{\iota, \sigma\}$, $\beta \in \{\iota, \sigma, \tau^3, \sigma\tau\}$ and $\gamma \in \{\iota, \sigma, \tau, \sigma\tau^3\}$. When M is a loop, its neutral element coincides with the neutral element of G.*

Proof. We first show that if M is a loop, its neutral element e coincides with the neutral element 1 of G. This is clear, as for some $\varepsilon \in A$ we have $1 = 1 * e = (1, e)\varepsilon \in \{e, e^{-1}\}$, and thus $1 = e$.

The equation $y = 1 * y$ holds for every $y \in G$ if and only if $y = (1, y)\alpha$, which happens if and only if $\alpha \in \{\iota, \sigma, \tau^3, \sigma\tau\}$. Similarly, the equation $y = y * 1$ holds for every $y \in G$ if and only if $\alpha \in \{\iota, \sigma, \tau, \sigma\tau^3\}$. Altogether, $y = y * 1 = 1 * y$ holds for every $y \in G$ if and only if $\alpha \in \{\iota, \sigma\}$.

Following the same strategy, $\overline{y} = 1 * \overline{y}$ holds for every $y \in G$ if and only if $\beta \in \{\iota, \sigma, \tau^3, \sigma\tau\}$, and $\overline{y} = \overline{y} * 1$ holds for every $y \in G$ if and only if $\gamma \in \{\iota, \sigma, \tau, \sigma\tau^3\}$. □

Once M is a loop, it must have two-sided inverses:

Lemma 3.2 *If M is a loop then it is an inverse property loop. In particular, if M happens to be a Bol loop, it must be Moufang.*

Proof. Assume that $x * y = 1$ for some $x, y \in G \cup \overline{G}$. Then both x, y belong to G, or both belong to $\overline{G}$, by Lemma 3.1. We therefore want to show that $(x, y)\varepsilon = 1$ implies $(y, x)\varepsilon = 1$ for every $\varepsilon \in A$ and $x, y \in G$.

Pick $\varepsilon \in A$. Then $(x, y)\varepsilon = (x^i y^j)^k$ for some $i, j, k \in \{-1, 1\}$. Assume that $(x, y)\varepsilon = 1$. Then $x^i y^j = 1$ and $y^j x^i = 1$. If $i = j$, we conclude from the latter equality that $y^i x^j = 1$, and thus $(y, x)\varepsilon = 1$. The inverse of the former equality yields $y^{-j} x^{-i} = 1$. If $i = -j$, we immediately have $y^i x^j = 1$, and thus $(y, x)\varepsilon = 1$.

Hence M is an inverse property loop. It is well-known that a Bol loop is Moufang if and only if it is an inverse property loop (cf. [15]). □

Given M as in (3.3), let

$$M^{\mathrm{op}} = \begin{pmatrix} \sigma\alpha & \sigma\gamma \\ \sigma\beta & \sigma\delta \end{pmatrix}.$$

Lemma 3.3 *The quasigroup M^{op} is opposite to M.*

Proof. Denote by $\circ$ the multiplication in M^{op}. Then

$$\begin{aligned} x \circ y &= (x, y)\sigma\alpha = (y, x)\alpha = y * x, \\ x \circ \overline{y} &= \overline{(x, y)\sigma\gamma} = \overline{(y, x)\gamma} = \overline{y} * x, \\ \overline{x} \circ y &= \overline{(x, y)\sigma\beta} = \overline{(y, x)\beta} = y * \overline{x}, \\ \overline{x} \circ \overline{y} &= (x, y)\sigma\delta = (y, x)\delta = \overline{y} * \overline{x}, \end{aligned}$$

for every x, $y \in G$. $\square$

Let us assume from now on that G *is nonabelian.* Then the identity $xy = yx$ and any other identity that reduces to $xy = yx$ do not hold in G, of course. We will come across the identity $xxy = yxx$. Note that this identity holds in G if and only if the center of G is of index 2 in G.

We would like to know when M is a Bol (and hence Moufang) loop. Assume from now on that M is a loop.

Recall that the opposite of a Moufang loop is again Moufang. We can therefore combine Lemmas 3.1, 3.3 and assume that the loop M satisfies $\alpha = \iota$. Since every Moufang loop is diassociative, we are going to have a look at such loops first:

Lemma 3.4 *If G is nonabelian and M is a diassociative loop with $\alpha = \iota$ then (β, γ, δ) is one of the eight triples*

$$\begin{array}{llll} (\iota,\iota,\iota), & (\tau^3,\iota,\sigma\tau), & (\sigma,\sigma,\sigma), & (\sigma\tau,\sigma,\tau^3), \\ (\tau^3,\tau,\tau^2), & (\iota,\tau,\sigma\tau^3), & (\sigma,\sigma\tau^3,\tau), & (\sigma\tau,\sigma\tau^3,\sigma\tau^2). \end{array} \tag{3.4}$$

Proof. The identities $(\overline{x} * \overline{x}) * y = \overline{x} * (\overline{x} * y)$, $\overline{x} * (y * \overline{x}) = (\overline{x} * y) * \overline{x}$ hold in M, for every x, $y \in G$. They translate into

$$(x,x)\delta y = (x,(x,y)\gamma)\delta, \tag{3.5}$$

$$(x,(y,x)\beta)\delta = ((x,y)\gamma,x)\delta, \tag{3.6}$$

respectively. We are first going to check which pairs (γ, δ) satisfy (3.5).

Assume that $\gamma = \iota$. Then (3.5) becomes $(x,x)\delta y = (x,xy)\delta$. Denote this identity by $I(\delta)$. Then $I(\iota)$ is $xxy = xxy$ (true), $I(\sigma)$ is $xxy = xyx$ (false), $I(\tau)$ is $y = y^{-1}$ (false), $I(\tau^2)$ is $x^{-2}y = x^{-1}y^{-1}x^{-1}$ (false), $I(\tau^3)$ is $y = xyx^{-1}$ (false), $I(\sigma\tau)$ is $y = y$ (true), $I(\sigma\tau^2)$ is $x^{-2}y = y^{-1}x^{-1}x^{-1}$ (false), and $I(\sigma\tau^3)$ is $y = xy^{-1}x^{-1}$ (false).

Assume that $\gamma = \sigma$. Then (3.5) becomes $(x,x)\delta y = (x,yx)\delta$. Verify that this identity holds only if $\delta = \sigma$ or $\delta = \tau^3$. (The case $\delta = \sigma$ leads to the identity $xxy = yxx$ mentioned before this lemma.)

When $\gamma = \tau$, (3.5) holds only if $\delta = \tau^2$ or $\delta = \sigma\tau^3$.

When $\gamma = \sigma\tau^3$, (3.5) holds only if $\delta = \tau$ or $\delta = \sigma\tau^2$.

Altogether, (3.5) can be satisfied only when (γ, δ) is one of the 8 pairs (ι,ι), $(\iota,\sigma\tau)$, (σ,σ), (σ,τ^3), (τ,τ^2), $(\tau,\sigma\tau^3)$, $(\sigma\tau^3,\tau)$, $(\sigma\tau^3,\sigma\tau^2)$. All these pairs will now be tested on (3.6).

Straightforward calculation shows that (3.6) can be satisfied only when (β, γ, δ) is one of the 8 triples listed in (3.4). $\square$

The Moufang identity $((xy)x)z = x(y(xz))$ will help us eliminate 4 out of the 8 possibilities in (3.4). We have $((x * \overline{y}) * x) * z = x * (\overline{y} * (x * z))$ in M, and thus

$$(((x,y)\beta,x)\gamma,z)\gamma = (x,(y,xz)\gamma)\beta. \tag{3.7}$$

The pairs $(\beta,\gamma) = (\sigma,\sigma)$, (τ^3,ι), (ι,τ), $(\sigma\tau,\sigma\tau^3)$ do not satisfy (3.7). For instance, $(\beta,\gamma) = (\sigma,\sigma)$ turns (3.7) into $zxyx = xzyx$, i.e., $zx = xz$.

The four remaining triples from (3.4) yield Moufang loops, as we are going to show.

The quadruple $(\iota, \iota, \iota, \iota) = G_\iota$ corresponds to the direct product of G and the two-element cyclic group. The quadruple $(\iota, \sigma, \sigma\tau^3, \tau) = M_c$ is the Chein Moufang loop $M(G, 2)$ that is associative if and only if G is abelian, by [11]. (We can also verify this directly.)

Set $G_\tau = (\iota, \tau^3, \tau, \tau^2)$ and $M_\sigma = (\iota, \sigma\tau, \sigma, \tau^3)$. We claim that G_ι is isomorphic to G_τ, and M_c is isomorphic to M_σ.

Lemma 3.5 *Define* $T : A^4 \longrightarrow A^4$ *by*

$$M = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \mapsto \begin{pmatrix} \alpha & \tau^3\beta \\ \gamma\tau & \tau^2\delta \end{pmatrix} = MT.$$

If $((x, y)\beta\Delta)^{-1} = (y^{-1}, x^{-1})\beta\Delta$ *and* $((x, y)\gamma\Delta)^{-1} = (x^{-1}, y)\gamma\tau\Delta$ *then* M *is isomorphic to* MT*.*

Proof. Consider the permutation f of $G \cup \overline{G}$ defined by $f(x) = x$, $f(\overline{x}) = \overline{x^{-1}}$, for $x \in G$. Let $*$ be the multiplication in M and $\circ$ the multiplication in MT. We show that $(x * y)f = xf \circ yf$ for every x, $y \in G \cup \overline{G}$. With x, $y \in G$, we have

$$\begin{aligned} (x * y)f &= (x, y)\alpha\Delta f = (x, y)\alpha\Delta = x \circ y = xf \circ yf, \\ (\overline{x} * \overline{y})f &= (x, y)\delta\Delta f = (x, y)\delta\Delta = (x^{-1}, y^{-1})\tau^2\delta\Delta = \overline{x}f \circ \overline{y}f. \end{aligned}$$

Using the assumption on β and γ, we also have

$$(x * \overline{y})f = \overline{(x, y)\beta\Delta}f = \overline{((x, y)\beta\Delta)^{-1}} = \overline{(y^{-1}, x^{-1})\beta\Delta} = \overline{(x, y^{-1})\tau^3\beta\Delta} = xf \circ \overline{y}f,$$

and

$$(\overline{x} * y)f = \overline{(x, y)\gamma\Delta}f = \overline{((x, y)\gamma\Delta)^{-1}} = \overline{(x^{-1}, y)\gamma\tau\Delta} = \overline{x}f \circ yf.$$

□

Note that $G_\iota T = G_\tau$ and $M_c T = M_\sigma$. Now, $\beta \in \{\iota, \sigma\}$ satisfies $((x, y)\beta\Delta)^{-1} = (y^{-1}, x^{-1})\beta\Delta$, and $\gamma \in \{\iota, \sigma\tau^3\}$ satisfies $((x, y)\gamma\Delta)^{-1} = (x^{-1}, y)\gamma\tau\Delta$. By Lemma 3.5, G_ι is isomorphic to G_τ, and M_c is isomorphic to M_σ.

We have proved:

Theorem 3.6 *Let* G *with* $|G| > 1$ *be a finite group that is not an elementary abelian* 2*-group. With the above conventions, let*

$$M = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix}$$

specify the multiplication in $L = G \cup \overline{G}$*, where* α*,* β*,* γ*,* $\delta \in A = \langle \sigma, \tau \rangle$*, and* $(x, y)\sigma = (y, x)$*,* $(x, y)\tau = (y^{-1}, x)$*. If* L *is a Bol loop then it is Moufang.*

When G is nonabelian, then L is a Bol loop if and only if M is equal to one of the following matrices:

$$
\begin{aligned}
G_\iota &= \begin{pmatrix} \iota & \iota \\ \iota & \iota \end{pmatrix}, & G_\iota^{op} &= \begin{pmatrix} \sigma & \sigma \\ \sigma & \sigma \end{pmatrix}, \\
G_\tau &= \begin{pmatrix} \iota & \tau^3 \\ \tau & \tau^2 \end{pmatrix}, & G_\tau^{op} &= \begin{pmatrix} \sigma & \sigma\tau \\ \sigma\tau^3 & \sigma\tau^2 \end{pmatrix}, \\
M_c &= \begin{pmatrix} \iota & \sigma \\ \sigma\tau^3 & \tau \end{pmatrix}, & M_c^{op} &= \begin{pmatrix} \sigma & \tau^3 \\ \iota & \sigma\tau \end{pmatrix}, \\
M_\sigma &= \begin{pmatrix} \iota & \sigma\tau \\ \sigma & \tau^3 \end{pmatrix}, & M_\sigma^{op} &= \begin{pmatrix} \sigma & \iota \\ \tau & \sigma\tau^3 \end{pmatrix}.
\end{aligned}
$$

The loops X^{op} are opposite to the loops X. The isomorphic loops G_ι, G_τ and their opposites are groups. The isomorphic loops M_c, M_σ and their opposites are Moufang loops that are not associative. The situation is depicted in Figures 3.1 *and* 3.2.

$$
\begin{array}{ccc}
G_\iota = \begin{pmatrix} \iota & \iota \\ \iota & \iota \end{pmatrix} & \xrightarrow{\text{op}} & G_\iota^{\text{op}} = \begin{pmatrix} \sigma & \sigma \\ \sigma & \sigma \end{pmatrix} \\
{\scriptstyle T}\downarrow{\scriptstyle \cong} & & \\
G_\tau = \begin{pmatrix} \iota & \tau^3 \\ \tau & \tau^2 \end{pmatrix} & \xrightarrow{\text{op}} & G_\tau^{\text{op}} = \begin{pmatrix} \sigma & \sigma\tau \\ \sigma\tau^3 & \sigma\tau^2 \end{pmatrix}
\end{array}
$$

Figure 3.1: All groups obtained in Theorem 3.6.

$$
\begin{array}{ccc}
M_c = \begin{pmatrix} \iota & \sigma \\ \sigma\tau^3 & \tau \end{pmatrix} & \xrightarrow{\text{op}} & M_c^{\text{op}} = \begin{pmatrix} \sigma & \tau^3 \\ \iota & \sigma\tau \end{pmatrix} \\
{\scriptstyle T}\downarrow{\scriptstyle \cong} & & \\
M_\sigma = \begin{pmatrix} \iota & \sigma\tau \\ \sigma & \tau^3 \end{pmatrix} & \xrightarrow{\text{op}} & M_\sigma^{\text{op}} = \begin{pmatrix} \sigma & \iota \\ \tau & \sigma\tau^3 \end{pmatrix}
\end{array}
$$

Figure 3.2: All nonassociative Moufang loops obtained in Theorem 3.6.

3.1.3 The abelian case

We prove in this subsection that even when G is abelian there are no additional constructions, besides those mentioned in Theorem 3.6, producing Bol loops (associative or nonassociative).

Assume that G is an abelian group with $|G| > 1$ that is not an elementary abelian 2-group. Then the group A of multiplications reduces to $A = \{\iota = \sigma, \tau = \sigma\tau^3, \tau^2 = \sigma\tau^2, \tau^3 = \sigma\tau\}$.

Lemmas 3.1 and 3.2 then show that M is a loop if and only if $\alpha = \iota$, $\beta \in \{\iota, \tau^3\}$, $\gamma \in \{\iota, \tau\}$ and $\delta \in \{\iota, \tau, \tau^2, \tau^3\}$.

Lemma 3.7 *Assume that G is an abelian group with $|G| > 1$ that is not an elementary abelian 2-group. If M is a diassociative loop then (β, γ, δ) is one of the triples*

$$(\iota, \iota, \iota), \quad (\iota, \tau, \tau), \quad (\tau^3, \iota, \tau^3), \quad (\tau^3, \tau, \tau^2). \tag{3.8}$$

Proof. Assume that M is a diassociative loop. Consider the identity (3.5). It becomes $y = xx^{-1}y^{-1}$ when $(\gamma, \delta) = (\iota, \tau)$, $x^{-2}y = x^{-2}y^{-1}$ when $(\gamma, \delta) = (\iota, \tau^2)$, and $y = x^{-1}xy^{-1}$ when $(\gamma, \delta) = (\tau, \tau^3)$.

Now consider the identity (3.6). It becomes $x^{-1}yx = x^{-1}y^{-1}x$ when $(\beta, \gamma, \delta) = (\iota, \iota, \tau^3)$, $x^{-1}y^{-1}x^{-1} = x^{-1}yx^{-1}$ when $(\beta, \gamma, \delta) = (\iota, \tau, \tau^2)$, $xy^{-1}x^{-1} = xyx$ when $(\beta, \gamma, \delta) = (\tau^3, \iota, \iota)$, and $xyx^{-1} = x^{-1}yx^{-1}$ when $(\beta, \gamma, \delta) = (\tau^3, \tau, \tau)$.

All of the above triples therefore do not yield a diassociative loop. The remaining triples (β, γ, δ) that yield a loop are listed in (3.8). □

Of course, the four triples (β, γ, δ) listed in (3.8) can already be found in Theorem 3.6. Namely, (ι, ι, ι) is a part of G_ι, (ι, τ, τ) is a part of M_c, (τ^3, ι, τ^3) is a part of M_σ, and (τ^3, τ, τ^2) is a part of G_τ. The Moufang loop M_c is a group if and only if G is abelian, as we have pointed out several times. Since $M_\sigma = M_c^{\mathrm{op}}$ when G is abelian, we are done.

3.2 Presentations for loops M(G,2)

In order to derive a presentation for a groupoid $A = (A, \cdot)$, one usually needs to introduce a normal form for elements of A written in terms of some generators. Such a normal form is not easy to find when A is not commutative, and even more so when A is not associative. Once a normal form is found, it might be still difficult to come up with presenting relations. Indeed, it is often the case that the only known presentation for a nonassociative groupoid is the *table presentation*, i.e., the presentation consisting of all relations $x \cdot y = z$ such that $x \cdot y$ equals z in A, and where x, y run over all elements of A. Table presentations are extremely useful when one constructs a multiplication table for A, however, they are of little use when one needs to identify A as a subgroupoid of another groupoid. To do the latter, it is necessary, in principle, to evaluate all products $x \cdot y$ with x, $y \in A$. It is therefore desirable to have access to presentations with a few presenting relations.

The infinite class of Moufang loops $M(G, 2)$ represents a significant portion of nonassociative Moufang loops of small order. We derive compact presentations for $M(G, 2)$ for every finite, two-generated group G.

3.2.1 Abundance of loops $M(G, 2)$

Besides the identity mentioned in the introduction, Moufang loops can be characterized by any of the equivalent *Moufang identities*

$$xy \cdot zx = x(yz \cdot x), \quad x(y \cdot xz) = (xy \cdot x)z, \quad x(y \cdot zy) = (xy \cdot z)y. \tag{3.9}$$

Recall that every element x of a Moufang loop has a two-sided inverse x^{-1}, and that Moufang loops are diassociative, i.e, every two-generated subloop is a group. We will use these well-known properties of Moufang loops without warning throughout this section.

Let us restate Chein's construction (3.1) once more. Let G be a finite group. Pick a new element u, and define

$$M(G, 2) = \{gu^\alpha;\ g \in G,\ \alpha = 0, 1\},$$

where

$$gu^\alpha \cdot hu^\beta = (g^{(-1)^\beta} h^{(-1)^{\alpha+\beta}})^{(-1)^\beta} u^{\alpha+\beta} \quad (g, h \in G,\ \alpha, \beta = 0, 1). \tag{3.10}$$

Again, $M(G, 2)$ is a Moufang loop that is associative if and only if G is abelian.

Let $\pi(m)$ be the number of isomorphism types of nonassociative Moufang loops of order at most m, and let $\sigma(m)$ be the number of nonassociative loops of the form $M(G, 2)$ of order at most m. Then, according to Chein's classification [11], $\pi(31) = 13$, $\sigma(31) = 8$, $\pi(63) = 158$, $\sigma(63) = 50$. (As Orin Chein kindly notified me, Edgar Goodaire noticed that the loop $M(S_3, 2) \times C_3$ is missing in [11]. Goodaire and his students also observed that $M_{48}(5, 5, 5, 3, 3, 0)$ is isomorphic to $M_{48}(5, 5, 5, 3, 6, 0)$, and $M_{48}(5, 5, 5, 3, 3, 6)$ to $M_{48}(5, 5, 5, 3, 6, 6)$. That is why $\pi(63)$ equals 158, rather than 159.) This demonstrates eloquently the abundance of loops of type $M(G, 2)$ among Moufang loops of small order.

3.2.2 Presentations

We start with the table presentation (3.10) for $M(G, 2)$ and prove:

Theorem 3.8 *Let $G = \langle x, y;\ R\rangle$ be a presentation for a finite group G, where R is a set of relations in generators x, y. Then $M(G, 2)$ is presented by*

$$\langle x, y, u;\ R,\ u^2 = (xu)^2 = (yu)^2 = (xy \cdot u)^2 = 1\rangle, \tag{3.11}$$

where 1 is the neutral element of G.

Let us emphasize that (3.11) is a presentation in the *variety of Moufang loops*, not groups.

The complicated multiplication formula (3.10) merely describes the four cases

$$\begin{aligned} g \cdot h &= gh, && (3.12)\\ gu \cdot h &= gh^{-1} \cdot u, && (3.13)\\ g \cdot hu &= hg \cdot u, && (3.14)\\ gu \cdot hu &= h^{-1}g && (3.15) \end{aligned}$$

in a compact way. In particular, identities (3.15) and (3.13) imply

$$u^2 = 1, \;\; gu = ug^{-1} \; (g \in G). \tag{3.16}$$

We claim that (3.16) is equivalent to (3.10). An element $g \in G$ will be called *good* if $gu = ug^{-1}$ can be derived from (3.11).

Lemma 3.9 *If $h \in G$ is good, then* (3.13) *holds. If g, h, $hg \in G$ are good, then* (3.14) *holds. If g, $g^{-1}h$ are good, then* (3.15) *holds.*

Proof. We have $gu \cdot h = (gu \cdot h)u \cdot u = (g \cdot uhu)u = (g \cdot h^{-1}uu)u = gh^{-1} \cdot u$ if h is good. Assume that g, h, hg are good. Then $g \cdot hu = g \cdot uh^{-1} = u \cdot u(g \cdot uh^{-1}) = u(ugu \cdot h^{-1}) = u \cdot g^{-1}h^{-1} = hg \cdot u$. Finally, when g and $g^{-1}h$ are good, we derive $gu \cdot hu = ug^{-1} \cdot hu = u \cdot g^{-1}h \cdot u = h^{-1}g$. □

Thus (3.16) is equivalent to (3.10). Moreover, in order to prove Theorem 3.8, it suffices to show that every $g \in G$ is good.

Thanks to diassociativity, g^s (s positive integer) is good whenever g is. Since G is finite, g^{-1} is good whenever g is.

Lemma 3.10 *Assume that g, $h \in G$ are good. Then gh is good if and only if hg is.*

Proof. Because of the symmetry, it is enough to prove only one implication. Assume that hg is good. By Lemma 3.9, $g \cdot hu = hg \cdot u$. Using this identity, we obtain $g \cdot hu \cdot g = (hg \cdot u)g$, $gh \cdot ug = h \cdot gug = hu$, $gh = hu \cdot g^{-1}u = uh^{-1} \cdot g^{-1}u = u \cdot h^{-1}g^{-1} \cdot u$, and so $gh \cdot u = u \cdot h^{-1}g^{-1}$. □

Lemma 3.11 *Assume that g, $h \in G$ are good. Then so is ghg.*

Proof. Since g^{-1}, h are good, Lemma 3.9 yields $ug \cdot h = g^{-1}u \cdot h = g^{-1}h^{-1} \cdot u$. Then $u \cdot ghg \cdot u = (ug \cdot h)g \cdot u = (g^{-1}h^{-1} \cdot u)g \cdot u = g^{-1}h^{-1} \cdot ugu = g^{-1}h^{-1}g^{-1}$, and we are done. □

We continue by induction on the *complexity*, or *length*, if you will, of the elements of G, defined below.

For $\varepsilon = 1, -1$, let X_ε be the set of symbols $\{x_1^\varepsilon, \cdots, x_m^\varepsilon\}$, and write $X = X_1 \cup X_{-1}$. Every word w of the free group $F = \langle X \rangle$ can be written uniquely in the form $x_{i_1}^{\varepsilon_1} \cdots x_{i_r}^{\varepsilon_r}$, where $i_j \neq i_{j+1}$, and ε_j is a nonzero integer. Define the *complexity* of w as the ordered pair $c(w) = (r, \sum_{j=1}^{r} |\varepsilon_r|)$, and order the complexities lexicographically.

From now on, assume that G is 2-generated, and write $x = x_1$, $y = x_2$.

Since $xu = ux^{-1}$ and $yu = uy^{-1}$ are presenting relations, both x, y are good, and hence both x^s, y^s are good for every integer s. The last presenting relation $xy \cdot u = u \cdot y^{-1}x^{-1}$ shows that both xy and $y^{-1}x^{-1} = (xy)^{-1}$ are good. Then yx and $x^{-1}y^{-1} = (yx)^{-1}$ are good, by Lemma 3.10. Also, Lemma 3.11 implies that $x^{-1} \cdot xy \cdot x^{-1} = yx^{-1}$ is good. Then $x^{-1}y$, $xy^{-1} = (yx^{-1})^{-1}$ and $y^{-1}x = (x^{-1}y)^{-1}$ are good, by Lemma 3.10. This means that every $g \in G$ with $c(g) < (2, 3)$ is good.

Lemma 3.12 *Every $g \in G$ with $c(g) < (3, 0)$ is good.*

Proof. Suppose there is g that is not good, and let $c(g) = (r, s)$ be as small as possible. We can assume that $g = a^u b^v$, where $\{a, b\} = \{x, y\}$, $s = |u| + |v| > 2$, and $u \neq 0 \neq v$.

Either $|u| > 1$ or $|v| > 1$. Without loss of generality, $u > 1$. (By Lemma 3.10, we can assume that $|u| > 1$. When u is negative, consider the inverse $b^{-v}a^{-u}$ instead, and apply Lemma 3.10 again.) Since $c(a^{u-2}b^v) < (2, s)$, the element $a^{u-2}b^v$ is good, and so is $a^{u-1}b^v a = a \cdot a^{u-2}b^v \cdot a$. As $a^{u-1}b^v$ is good by the induction hypothesis, $a^u b^v a = a \cdot a^{u-1}b^v \cdot a$ is good as well, by Lemma 3.11. Then the decomposition of $a^{u-1}b^v a$ into $a^{-1} \cdot a^u b^v a$ demonstrates that $a^u b^v a \cdot a^{-1} = a^u b^v$ is good, by Lemma 3.10. We have reached a contradiction. □

To finish the proof, assume there is $g \in G$ that is not good, and let $c(g) = (r, s)$ be as small as possible. By Lemma 3.12, $r \geq 3$. When r is odd, we can write $g = a^{\varepsilon_1}b^{\varepsilon_2}a^{\varepsilon_3} \cdots b^{\varepsilon_{r-1}}a^{\varepsilon_r} = khk$, where $k = a^{\varepsilon_r}$, $h = a^{\varepsilon_1 - \varepsilon_r}b^{\varepsilon_2}a^{\varepsilon_3} \cdots b^{\varepsilon_{r-1}}$, and $\{a, b\} = \{x, y\}$. Since $c(k)$, $c(h) < (r, s)$, both k, h are good, and then g is good by Lemma 3.11.

Assume that r is even. Then $g = a^{\varepsilon_1}b^{\varepsilon_2} \cdots a^{\varepsilon_{r-1}}b^{\varepsilon_r} = khk$, where $k = a^{\varepsilon_1}b^{\varepsilon_r}$, $h = b^{\varepsilon_2 - \varepsilon_r}a^{\varepsilon_3} \cdots b^{\varepsilon_{r-2}}a^{\varepsilon_{r-1} - \varepsilon_1}$. Again, $c(k)$, $c(h) < (r, s)$, thus both k and h are good, and so is g, by Lemma 3.11.

Theorem 3.8 is proved.

3.3 The smallest Moufang loop

Thirty years ago, Chein and Pflugfelder [14] proved that the smallest nonassociative Moufang loop is of order 12 and is unique up to isomorphism. It coincides with $M = M(S_3, 2)$. Guided by our presentation for M, we give a new, visual description of M in the last section. The multiplication formula (3.10) for M is certainly difficult to memorize, and so is the one in [45, Example IV.1.2].

Note that there are 9 involutions and 2 elements of order 3 in M (cf. [10, Table 3]). We are going to define a 12-element groupoid L and show that it is isomorphic to M.

Look at the four diagrams in Figure 3.3. Think of the vertices $x_0, \ldots, x_8$ as involutions. Let L consist of e, $x_0, \ldots, x_8$, y, y^{-1}, where y is of order 3. Interpret the edges of diagrams I–IV as multiplication rules in the following way. If x_i and x_j are connected by a solid line, let $x_i x_j$ be the third vertex of the (unique) triangle

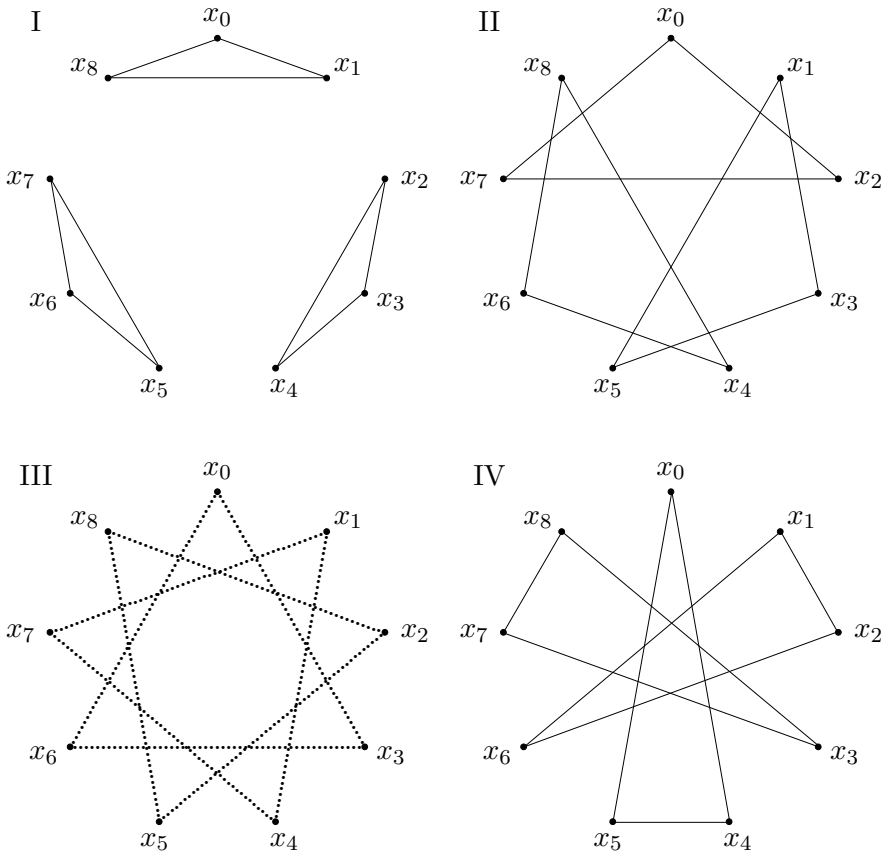

Figure 3.3: Multiplication in $M(S_3, 2)$

containing both x_i and x_j. If x_i and x_j are not connected by a solid line, we must have $j = i \pm 3$, and then x_i and x_j are connected by a dotted line (in diagram III). Define $x_i x_{i+3} = y$ and $x_i x_{i-3} = y^{-1}$.

This partial multiplication can be extended by properties of Moufang loops. To avoid ambiguity, we postulate that $x_i y = y^{-1} x_i = x_{i+3}$ and $y x_i = x_i y^{-1} = x_{i-3}$. For the convenience of the reader, we give a multiplication table of M in Table 3.1.

Obviously, L is closed under multiplication and has a neutral element. It is nonassociative, since $x_0 x_1 \cdot x_3 = x_8 x_3 = x_7 \neq x_4 = x_0 x_5 = x_0 \cdot x_1 x_3$. Is L isomorphic to M? There is a unique Moufang loop of order 12 [14], so it suffices to check the Moufang identities for L. However, this is not so easy! Instead, we verify directly that L satisfies the multiplication formula (3.10) with some choice of G and u.

Remark 3.13 *It does not suffice to verify* (3.16) *for some choice of* G *and* u *because* (3.16) *is equivalent to* (3.10) *only when it is assumed that* L *is Moufang.*

Put $x = x_0$, and observe that $G = \langle x, y \rangle = \{1, x_0, y, x_3, x_6, y^{-1}\}$ is isomorphic

Table 3.1: Multiplication table of $M(S_3, 2)$.

	1	x_0	x_1	x_2	x_3	x_4	x_5	x_6	x_7	x_8	y	y^{-1}
1	1	x_0	x_1	x_2	x_3	x_4	x_5	x_6	x_7	x_8	y	y^{-1}
x_0	x_0	1	x_8	x_7	y	x_5	x_4	y^{-1}	x_2	x_1	x_3	x_6
x_1	x_1	x_8	1	x_6	x_5	y	x_3	x_2	y^{-1}	x_0	x_4	x_7
x_2	x_2	x_7	x_6	1	x_4	x_3	y	x_1	x_0	y^{-1}	x_5	x_8
x_3	x_3	y^{-1}	x_5	x_4	1	x_2	x_1	y	x_8	x_7	x_6	x_0
x_4	x_4	x_5	y^{-1}	x_3	x_2	1	x_0	x_8	y	x_6	x_7	x_1
x_5	x_5	x_4	x_3	y^{-1}	x_1	x_0	1	x_7	x_6	y	x_8	x_2
x_6	x_6	y	x_2	x_1	y^{-1}	x_8	x_7	1	x_5	x_4	x_0	x_3
x_7	x_7	x_2	y	x_0	x_8	y^{-1}	x_6	x_5	1	x_3	x_1	x_4
x_8	x_8	x_1	x_0	y	x_7	x_6	y^{-1}	x_4	x_3	1	x_2	x_5
y	y	x_6	x_7	x_8	x_0	x_1	x_2	x_3	x_4	x_5	y^{-1}	1
y^{-1}	y^{-1}	x_3	x_4	x_5	x_6	x_7	x_8	x_0	x_1	x_2	1	y

to S_3. Let $u = x_1 \notin G$. We show that (3.12)–(3.15) are satisfied for every g, $h \in G$. Thanks to the symmetry of Figure 3.3, it is enough to consider only $\{g, h\} = \{x_0, x_3\}$, $\{x_0, y\}$.

Identity (3.12) is trivial. Let us prove (3.13). We have $x_0x_1 \cdot x_3 = x_8x_3 = x_7 = yx_1 = x_0x_3^{-1} \cdot x_1$, $x_0x_1 \cdot y = x_8y = x_2 = x_6x_1 = x_0y^{-1} \cdot x_1$, $x_3x_1 \cdot x_0 = x_5x_0 = x_4 = y^{-1}x_1 = x_3x_0^{-1} \cdot x_1$, and $yx_1 \cdot x_0 = x_7x_0 = x_2 = x_6x_1 = yx_0^{-1} \cdot x_1$. Similarly for (3.14), (3.15).

Hence L is isomorphic to M. The subloop structure of L is apparent from the visual rules, too. If $j \equiv i \pmod 3$ then $\langle x_i, x_j \rangle \cong S_3$; otherwise, $\langle x_i, x_j \rangle \cong V_4$, for $i \neq j$.

Chapter 4

Simple Moufang Loops

Moufang loops are one of the best-known generalizations of groups. As in any variety, one is especially interested in simple and subdirectly irreducible objects.

There is a countable family of nonassociative simple Moufang loops, arising from split octonion algebras. We will call them *Paige loops*, after their discoverer. We prove that every finite Paige loop is generated by three elements, using the classical results on generators of unimodular groups. In Section 4.2, we find the automorphism groups of all Paige loops constructed over perfect fields. Results of Section 4.1 appeared (will appear) in [55], [57] and [56]. Section 4.2 is based on [42], a paper written with Gábor P. Nagy.

4.1 Generators for Paige loops

The most famous Moufang loop is the multiplicative loop of nonzero elements in the standard 8-dimensional real octonion algebra $\mathbb{O}$. Surely the best-known *finite* Moufang loop is the 240-element loop L of integral octonions of norm one [16].

In 1956, Paige [44] found one nonassociative simple Moufang loop for every field. Following Bannai and Song [6], we denote this *Paige loop* constructed over F by $M^*(F)$. Let us give a brief description of $M^*(F)$ now.

Consider the Zorn multiplication

$$\begin{pmatrix} a & \alpha \\ \beta & b \end{pmatrix} \begin{pmatrix} c & \gamma \\ \delta & d \end{pmatrix} = \begin{pmatrix} ac + \alpha \cdot \delta & a\gamma + \alpha d - \beta \times \delta \\ \beta c + b\delta + \alpha \times \gamma & \beta \cdot \gamma + bd \end{pmatrix}, \qquad (4.1)$$

where a, b, c, $d \in F$, α, β, γ, $\delta \in F^3$, and where $\alpha \cdot \delta$ (resp. $\alpha \times \delta$) denotes the dot product (resp. cross product) of α and δ. This is the same formula Zorn used to construct the split octonion algebra over F. (See Section 4.2 for more information on octonion algebras.) The loop $M^*(F)$ consists of all matrices

$$M = \begin{pmatrix} a & \alpha \\ \beta & b \end{pmatrix}$$

with $\det M = ab - \alpha\beta = 1$ that are multiplied according to (4.1), and where M and $-M$ are identified. The neutral element of $M^*(F)$ is the identity matrix I, and the inverse of M is

$$M^{-1} = \begin{pmatrix} b & -\alpha \\ -\beta & a \end{pmatrix}.$$

In 1987, Liebeck [38] proved that there are no other nonassociative finite simple Moufang loops, besides the loops $M^*(GF(q)) = M^*(q)$. (See [43] for a thorough discussion of this topic.) The loop $M^*(2)$ is exceptional in the sense that it shows up in the real octonion algebra $\mathbb{O}$, too. Namely, $M^*(2)$ is isomorphic to the quotient of L by its center $Z(L) = \{1, -1\}$, cf. [16].

Associative finite simple Moufang loops are finite simple groups. It is a remarkable fact that every finite simple group is 2-generated [3]; even more so, since no proof using only the simplicity is known. Instead, every family of finite simple groups must be investigated separately. Because of diassociativity, the nonassociative Paige loops cannot be 2-generated. It is reasonable to expect that a small number of generators will do. Indeed, it this section we prove that:

Theorem 4.1 *Every nonassociative finite simple Moufang loop is* 3*-generated.*

Note that Theorem 4.1 was proved in [57] for all Paige loops $M^*(p)$, p a prime. Thus the main task of this section is to cover the general case. Nevertheless, we also present a simple proof for the prime case, and offer at least two generating sets for every $M^*(q)$.

4.1.1 Generators for $L_2(q)$

The crucial observation concerning Paige loops is that $M^*(q)$ contains several copies of $L_2(q) = PSL_2(q)$. Given the canonical basis $e_1 = (1, 0, 0)$, $e_2 = (0, 1, 0)$, $e_3 = (0, 0, 1)$ of F^3, let $\phi_i : L_2(q) \longrightarrow M^*(q)$ be defined by

$$\phi_i \begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} a & be_i \\ ce_i & d \end{pmatrix},$$

and let G_i be the image of $L_2(q)$ under ϕ_i. Since the multiplication in G_i coincides with the usual matrix multiplication (all cross products involved in (4.1) vanish), ϕ_i is an isomorphism $L_2(q) \longrightarrow G_i$.

This brings our attention to the classical results concerning generators for $L_2(q)$ and $SL_2(q)$. First of all, we have the Dickson Theorem:

Theorem 4.2 (Dickson, 1900) *If $q \neq 9$ is an odd prime power or $q = 2$, then $SL_2(q)$ is generated by*

$$\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, \quad \begin{pmatrix} 1 & 0 \\ \lambda & 1 \end{pmatrix}, \tag{4.2}$$

where λ is a primitive element of $GF(q)$.

The proof can be found in [18], and more recently in [30, pp. 44–55]. The statement of the theorem usually does not mention $q = 2$, although it is apparently true for $q = 2$, since $SL_2(2) \cong S_3$ is generated by any two involutions, in particular by (4.2).

A. A. Albert and J. Thompson proved [1, Lemma 8] that for any primitive element λ of $GF(q)$, $q > 2$, the group $SL_2(q)$ is generated by B, $-B$, and C, where

$$B = \begin{pmatrix} \lambda & 0 \\ 0 & \lambda^{-1} \end{pmatrix}, \quad C = \begin{pmatrix} 0 & 1 \\ -1 & \lambda \end{pmatrix}. \tag{4.3}$$

We therefore have:

Proposition 4.3 (Albert, Thompson, 1959) *Let q be a prime power bigger than 2. Then $L_2(q)$ is generated by (4.3), where λ is a primitive element of $GF(q)$.*

The generators (4.3) are especially convenient for our purposes, because $\phi_i(B) = B$ for every i, $1 \leq i \leq 3$; but let us not get ahead of ourselves. It is practical to know some generators that do not involve a primitive element. For that matter, Coxeter and Moser argue in [17] that

Lemma 4.4 *For every prime p, the group $L_2(p)$ is generated by*

$$\begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}, \quad \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}. \tag{4.4}$$

4.1.2 Generators for $M^*(q)$

Our first result concerning $M^*(q)$ has nothing to do with the generators for $L_2(q)$. In its proof, we take advantage of the following lemma due to Paige:

Lemma 4.5 (Paige, 1956) *$M^*(q)$ is generated by*

$$M_\beta = \begin{pmatrix} 1 & 0 \\ \beta & 1 \end{pmatrix}, \quad M'_\beta = \begin{pmatrix} 1 & \beta \\ 0 & 1 \end{pmatrix}, \tag{4.5}$$

where β runs over all nonzero vectors in F^3.

Proof. Combine Lemmas 4.2 and 4.3 of [44]. □

Proposition 4.6 *$M^*(q)$ is generated by $G_1 \cup G_2 \cup G_3$.*

Proof. Let Q be the subloop of $M^*(q)$ generated by $G_1 \cup G_2 \cup G_3$. Thanks to Lemma 4.5, it suffices to prove that Q contains all elements M_β, M'_β, defined in (4.5). We show simultaneously that $M_\beta \in Q$ and $M'_\beta \in Q$.

Let k denote the number of nonzero entries of β. There is nothing to prove when $k \leq 1$. Suppose that $k = 2$. Without loss of generality, let $\beta = (a, b, 0)$ for some a, $b \in F^* = F \setminus \{0\}$. Verify that

$$\begin{pmatrix} 1 & ae_1 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & be_2 \\ 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} 1 & 0 \\ -abe_3 & 1 \end{pmatrix} = \begin{pmatrix} 1 & (a,b,0) \\ 0 & 1 \end{pmatrix},$$

and thus that $M_\beta \in Q$. Similarly, $M'_\beta \in Q$. We can therefore assume that Q contains all elements M_β, M'_β with $k \leq 2$.

Let $k = 3$, $\beta = (a, b, c)$ for some $a, b, c \in F^*$. As

$$\begin{pmatrix} 1 & (a,b,0) \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & (0,0,c) \\ 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} 1 & 0 \\ (-bc,ac,0) & 1 \end{pmatrix} = \begin{pmatrix} 1 & (a,b,c) \\ 0 & 1 \end{pmatrix},$$

M_β belongs to Q. Symmetrically, $M'_\beta \in Q$, and we are done. □

In fact, $G_1 \cup G_2$ already generates $M^*(q)$. The role of the cross product is especially apparent in the next Proposition.

Proposition 4.7 *The subgroup G_3 is contained in the subloop of $M^*(q)$ generated by $G_1 \cup G_2$. In particular, $M^*(q)$ is generated by $G_1 \cup G_2$.*

Proof. As it turns out, all we need are these two equations:

$$\begin{pmatrix} 1 & 0 \\ \lambda e_3 & 1 \end{pmatrix} = - \begin{pmatrix} 0 & e_2 \\ -e_2 & 0 \end{pmatrix} \begin{pmatrix} 1 & \lambda e_1 \\ -\lambda^{-1} e_1 & 0 \end{pmatrix} \cdot \begin{pmatrix} 1 & e_2 \\ -e_2 & 0 \end{pmatrix} \begin{pmatrix} 1 & \lambda e_1 \\ -\lambda^{-1} e_1 & 0 \end{pmatrix},$$

and

$$\begin{pmatrix} 0 & e_3 \\ -e_3 & 0 \end{pmatrix} = \begin{pmatrix} 0 & e_1 \\ -e_1 & 0 \end{pmatrix} \begin{pmatrix} 0 & -e_2 \\ e_2 & 0 \end{pmatrix}.$$

Note that the left hand sides of these equations are elements of G_3, whereas the right hand sides are products of elements of $G_1 \cup G_2$. When $q = 2$, we are done by Lemma 4.4. When $q > 2$, observe that

$$\begin{pmatrix} 1 & 0 \\ \lambda & 1 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ -1 & \lambda \end{pmatrix} = C.$$

Since $B = \phi_i(B)$ for every i, $1 \leq i \leq 3$, we are done by Proposition 4.3. □

Theorem 4.1 is now proved. When $q > 2$, $M^*(q)$ is generated by $\phi_1(C)$, $\phi_2(C)$ and $B = \phi_1(B) = \phi_2(B)$, by Propositions 4.3 and 4.7. When $q = 2$, we are done by the main result of [57], Theorem 2.1 [57].

For the sake of completeness, allow us to present an alternative, simpler proof of [57, Theorem 2.1].

Proposition 4.8 [57, Theorem 2.1] *Let p be a prime. Then $M^*(p)$ is generated by*

$$U_1 = \begin{pmatrix} 1 & e_1 \\ 0 & 1 \end{pmatrix}, \quad U_2 = \begin{pmatrix} 1 & e_2 \\ 0 & 1 \end{pmatrix}, \quad X = \begin{pmatrix} 0 & e_3 \\ -e_3 & 1 \end{pmatrix}.$$

Proof. First check that

$$\begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}^{-1} \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}^{-1}. \tag{4.6}$$

Combine (4.4) and (4.6) to see that $L_2(p)$ is generated by

$$U = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, \ V = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}.$$

Consequently, $M^*(p)$ is generated by $U_1 = \phi_1(U)$, $U_2 = \phi_2(U)$, $V_1 = \phi_1(V)$, and $V_2 = \phi_2(V)$. Now,

$$\begin{aligned} V_2 &= -(XU_1 \cdot XU_2) \cdot X^{-1}U_1, \\ V_1 &= -U_1U_2 \cdot (V_2 \cdot U_1X), \end{aligned}$$

and we are through. □

4.1.3 Additional generating sets

We would like to show how to obtain additional generating sets for $M^*(q)$. We take advantage of Proposition 4.7, Dickson's Theorem, and of the fact that $SL_2(2^r)$ (for $r > 1$) is generated by

$$D_1 = \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}, \ D_2 = \begin{pmatrix} \lambda & 0 \\ 0 & \lambda^{-1} \end{pmatrix}, \tag{4.7}$$

where λ is a primitive element of $GF(2^r)$. We leave the verification of (4.7) to the reader. (Or see [55].)

Since $\phi_i(D_2) = D_2$ for $i = 1, 2, 3$, we immediately see from Proposition 4.7 that $M^*(2^r)$ (for $r > 1$) is generated by $\phi_1(D_1)$, $\phi_2(D_1)$ and D_2.

Proposition 4.9 *Let $q \neq 9$ be an odd prime power or $q = 2$. Then $M^*(q)$ is generated by*

$$\begin{pmatrix} 1 & e_1 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & e_2 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 0 & \lambda e_3 \\ -\lambda^{-1}e_3 & 1 \end{pmatrix},$$

where λ is a primitive element of $GF(q)$.

Proof. Keeping Proposition 4.7 and Dickson's Theorem in mind, we only need to obtain the elements

$$\begin{pmatrix} 1 & 0 \\ \lambda e_i & 1 \end{pmatrix},$$

for $i = 1, 2$. Straightforward computation reveals that

$$\begin{aligned} \begin{pmatrix} 1 & 0 \\ \lambda e_1 & 1 \end{pmatrix} &= -\begin{pmatrix} 0 & \lambda e_3 \\ -\lambda^{-1}e_3 & 1 \end{pmatrix}^2 \begin{pmatrix} 1 & e_2 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 0 & \lambda e_3 \\ -\lambda^{-1}e_3 & 1 \end{pmatrix}, \\ \begin{pmatrix} 1 & 0 \\ \lambda e_2 & 1 \end{pmatrix}^{-1} &= -\begin{pmatrix} 0 & \lambda e_3 \\ -\lambda^{-1}e_3 & 1 \end{pmatrix}^2 \begin{pmatrix} 1 & e_1 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 0 & \lambda e_3 \\ -\lambda^{-1}e_3 & 1 \end{pmatrix}. \end{aligned}$$

Note that the expressions on the right hand side can be evaluated in any order. □

4.2 Automorphism groups of Paige loops

As we hope to attract the attention of both group- and loop-theorists in this section, we take the risk of being trivial at times and introduce most of the background material carefully, although briefly. We refer the reader to [49], [45], [9] and [33] for a more systematic exposition.

Let C be a vector space over a field F, and $N : C \longrightarrow F$ a nondegenerate quadratic form. Define multiplication $\cdot$ on C so that $(C, +, \cdot)$ becomes a not necessarily associative ring. Then $C = (C, N)$ is a *composition algebra* if $N(u \cdot v) = N(u) \cdot N(v)$ holds for every $u, v \in C$. Composition algebras exist only in dimensions 1, 2, 4 and 8, and we speak of an *octonion algebra* when $\dim C = 8$. (See [48] for a generalization to dimension 16.) A composition algebra is called *split* when it has nontrivial zero divisors. By [49, Theorem 1.8.1], there is a unique split octonion algebra $\mathbb{O}F$ over any field F.

Write $(\mathbb{O}F)^*$ for the set of all elements of unit norm in $\mathbb{O}F$, and let $M^*(F)$ be the quotient of $(\mathbb{O}F)^*$ by its center $Z((\mathbb{O}F)^*) = \{\pm 1\}$. Since every composition algebra satisfies all Moufang identities, both $(\mathbb{O}F)^*$ and $M^*(F)$ are Moufang loops. As we have already pointed out in Section 4.1, Paige proved [44] that $M^*(F)$ is nonassociative and simple (as a loop), and Liebeck [38] used the classification of finite simple groups to conclude that there are no other nonassociative finite simple Moufang loops besides $M^*(q)$.

Liebeck's proof relies heavily on results of Doro [19], that relate Moufang loops to groups with triality. (We managed to avoid all of Doro's paper in [43].) Before we define these groups, allow us to say a few words about the (standard) notation. Let G be a group. Working in the holomorph $G \rtimes \mathrm{Aut}(G)$, when $g \in G$ and $\alpha \in \mathrm{Aut}(G)$, we write g^α for the image of g under α, and $[g, \alpha]$ for $g^{-1}g^\alpha$. Appealing to this convention, we say that α *centralizes* g if $g^\alpha = g$. Now, the pair (G, S) is said to be a *group with triality* if $S \leq \mathrm{Aut}(G)$, $S = \langle \sigma, \rho \rangle \cong S_3$, σ is an involution, ρ is of order 3, $G = [G, S]$, $Z(GS) = \{1\}$, and the triality equation

$$[g, \sigma][g, \sigma]^\rho[g, \sigma]^{\rho^2} = 1$$

holds for every $g \in G$.

We now turn to geometrical loop theory, an important part of the theory of loops (cf. [45], [41]). A 3-*net* is an incidence structure $\mathcal{N} = (\mathcal{P}, \mathcal{L})$ with point set $\mathcal{P}$ and line set $\mathcal{L}$, where $\mathcal{L}$ is a disjoint union of 3 classes $\mathcal{L}_i$ $(i = 1, 2, 3)$ such that two distinct lines from the same class have no point in common, and any two lines from distinct classes intersect in exactly one point. A line from the class $\mathcal{L}_i$ is usually referred to as an *i-line*. A permutation on $\mathcal{P}$ is a *collineation* of $\mathcal{N}$ if it maps lines to lines. We speak of a *direction preserving* collineation if the line classes $\mathcal{L}_i$ are invariant under the induced permutation of lines.

There is a canonical correspondence between loops and 3-nets. Any loop L determines a 3-net when we let $\mathcal{P} = L \times L$, $\mathcal{L}_1 = \{\{(c, y)|y \in L\}|c \in L\}$, $\mathcal{L}_2 = \{\{(x, c)|x \in L\}|c \in L\}$, $\mathcal{L}_3 = \{\{(x, y)|x, y \in L, xy = c\}|c \in L\}$. Conversely, given

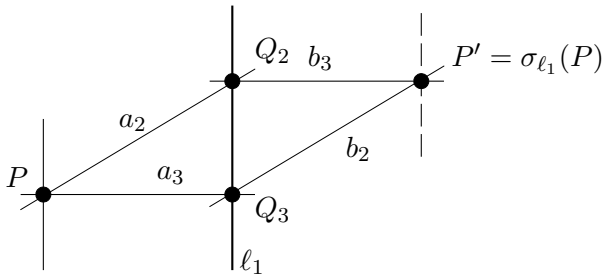

Figure 4.1: The Bol reflection with axis ℓ_1

a 3-net $\mathcal{N} = (\mathcal{P}, \mathcal{L})$ and the origin $1 \in \mathcal{P}$, we can introduce multiplication on the 1-line ℓ through 1 that turns ℓ into a loop, called the *coordinate loop* of $\mathcal{N}$. Since the details of this construction are not essential for what follows, we omit them.

Let $\mathcal{N}$ be a 3-net and $\ell_i \in \mathcal{L}_i$, for some i. We define a certain permutation σ_{ℓ_i} on the point set $\mathcal{P}$ (cf. Figure 4.1). For $P \in \mathcal{P}$, let a_j and a_k be the lines through P such that $a_j \in \mathcal{L}_j$, $a_k \in \mathcal{L}_k$, and $\{i, j, k\} = \{1, 2, 3\}$. Then there are unique intersection points $Q_j = a_j \cap \ell_i$, $Q_k = a_k \cap \ell_i$. We define $\sigma_{\ell_i}(P) = b_j \cap b_k$, where b_j is the unique j-line through Q_k, and b_k the unique k-line through Q_j. The permutation σ_{ℓ_i} is clearly an involution satisfying $\sigma_{\ell_i}(\mathcal{L}_j) = \mathcal{L}_k$, $\sigma_{\ell_i}(\mathcal{L}_k) = \mathcal{L}_j$. If it happens to be the case that σ_{ℓ_i} is a collineation, we call it the *Bol reflection with axis* ℓ_i.

It is clear that for any collineation γ of $\mathcal{N}$ and any line ℓ we have $\sigma_{\gamma(\ell)} = \gamma\sigma_\ell\gamma^{-1}$. Hence the set of Bol reflections of $\mathcal{N}$ is invariant under conjugations by elements of the collineation group $\mathrm{Coll}(\mathcal{N})$ of $\mathcal{N}$. A 3-net $\mathcal{N}$ is called a *Moufang 3-net* if σ_ℓ is a Bol reflection for every line ℓ. Bol proved that $\mathcal{N}$ is a Moufang 3-net if and only if all coordinate loops of $\mathcal{N}$ are Moufang (cf. [8, p. 120]).

We are now coming to the crucial idea of this section. For a Moufang 3-net $\mathcal{N}$ with origin 1, denote by ℓ_i ($i = 1, 2, 3$) the three lines through 1. As in [33], we write Γ_0 for the subgroup of $\mathrm{Coll}(N)$ generated by all Bol reflections of $\mathcal{N}$, and Γ for the direction preserving part of Γ_0. Also, let S be the subgroup generated by σ_{ℓ_1}, σ_{ℓ_2} and σ_{ℓ_3}. According to [33], Γ is a normal subgroup of index 6 in Γ_0, $\Gamma_0 = \Gamma S$, and (Γ, S) is a group with triality. (Here, S is understood as a subgroup of $\mathrm{Aut}(\Gamma)$ by identifying $\sigma \in S$ with the map $\tau \mapsto \sigma\tau\sigma^{-1}$.) We will always fix $\sigma = \sigma_{\ell_1}$ and $\rho = \sigma_{\ell_1}\sigma_{\ell_2}$ in such a situation, to obtain $S = \langle\sigma, \rho\rangle$ as in the definition of a group with triality.

4.2.1 The automorphisms

Let V be a vector space over F. Then $f : V \longrightarrow V$ is *F-semilinear* if there is $\alpha \in \mathrm{Aut}(F)$ such that $f(u+v) = f(u) + f(v)$ and $f(\lambda u) = \alpha(\lambda) f(u)$ for every u, $v \in V$ and $\lambda \in F$.

Let C be a composition algebra over F. A map $\alpha : C \longrightarrow C$ is a *linear automorphism* (resp. *semilinear automorphism*) of C if it is a bijective F-linear (resp. F-semilinear) map preserving the multiplication, i.e., satisfying $\alpha(uv) = \alpha(u)\alpha(v)$ for every u, $v \in C$. It is well known that the group of linear automorphisms of $\mathbb{O}F$ is isomorphic to the Chevalley group $G_2(F)$, cf. [27, Section 3], [49, Chapter 2]. The group of semilinear automorphisms of $\mathbb{O}F$ is therefore isomorphic to $G_2(F) \rtimes \mathrm{Aut}(F)$.

Since every linear automorphism of a composition algebra is an isometry [49, Section 1.7], it induces an automorphisms of the loop $M^*(F)$. By [55, Theorem 3.3], every element of $\mathbb{O}F$ is a sum of two elements of norm one. Consequently, $\mathrm{Aut}(\mathbb{O}F) \leq \mathrm{Aut}(M^*(F))$.

An automorphism $f \in \mathrm{Aut}(M^*(F))$ will be called *(semi)linear* if it is induced by a (semi)linear automorphism of $\mathbb{O}F$. By considering extensions of automorphisms of $M^*(F)$, it was proved in [55] that $\mathrm{Aut}(M^*(2))$ is isomorphic to $G_2(2)$. The aim of this section is to generalize this result (although using different techniques) and prove that every automorphism of $\mathrm{Aut}(M^*(F))$ is semilinear, provided F is perfect. We reach this aim by identifying $\mathrm{Aut}(M^*(F))$ with a certain subgroup of the automorphism group of the group with triality associated with $M^*(F)$.

To begin with, we recall the geometrical characterization of automorphisms of a loop.

Lemma 4.10 (Theorem 10.2 [7]) *Let L be a loop and $\mathcal{N}$ its associated 3-net. Any direction preserving collineation which fixes the origin of $\mathcal{N}$ is of the form $(x, y) \mapsto (x^\alpha, y^\alpha)$ for some $\alpha \in \mathrm{Aut}(L)$. Conversely, the map $\alpha : L \longrightarrow L$ is an automorphism of L if and only if $(x, y) \mapsto (x^\alpha, y^\alpha)$ is a direction preserving collineation of $\mathcal{N}$.*

We will denote the map $(x, y) \mapsto (x^\alpha, y^\alpha)$ by φ_α.

By [33, Propositions 3.3 and 3.4], $\mathcal{N}$ is embedded in $\Gamma_0 = \Gamma S$ as follows. The lines of $\mathcal{N}$ correspond to the conjugacy classes of σ in Γ_0, two lines are parallel if and only if the corresponding involutions are Γ-conjugate, and three pairwise non-parallel lines have a point in common if and only if they generate a subgroup isomorphic to S_3. In particular, the three lines through the origin of $\mathcal{N}$ correspond to the three involutions of S.

As the set of Bol reflections of $\mathcal{N}$ is invariant under conjugations by collineations, every element $\varphi \in \mathrm{Coll}(\mathcal{N})$ normalizes the group Γ and induces an automorphism $\widehat{\varphi}$ of Γ. It is not difficult to see that φ fixes the three lines through the origin of $\mathcal{N}$ if and only if $\widehat{\varphi}$ centralizes (the involutions of) S.

Proposition 4.11 *Let L be a Moufang loop and $\mathcal{N}$ its associated 3-net. Let Γ_0 be the group of collineations generated by the Bol reflections of $\mathcal{N}$, Γ the direction preserving*

part of Γ_0*, and* $S \cong S_3$ *the group generated by the Bol reflections whose axis contains the origin of* $\mathcal{N}$*. Then* $\mathrm{Aut}(L)$ *is isomorphic to* $C_{\mathrm{Aut}(\Gamma)}(S)$*, the centralizer of* S *in* $\mathrm{Aut}(\Gamma)$*.*

Proof. Pick $\alpha \in \mathrm{Aut}(L)$, and let $\widehat{\varphi_\alpha}$ be the automorphism of Γ induced by the collineation φ_α. As φ_α fixes the three lines through the origin, $\widehat{\varphi_\alpha}$ belongs to $C_{\mathrm{Aut}(\Gamma)}(S)$.

Conversely, an element $\psi \in C_{\mathrm{Aut}(\Gamma)}(S)$ normalizes the conjugacy class of σ in ΓS and preserves the incidence structure defined by the embedding of $\mathcal{N}$. This means that $\psi = \widehat{\varphi}$ for some collineation $\varphi \in \mathrm{Coll}(\mathcal{N})$. Now, ψ centralizes S, therefore φ fixes the three lines through the origin. Thus φ must be direction preserving, and there is $\alpha \in \mathrm{Aut}(L)$ such that $\varphi = \varphi_\alpha$, by Lemma 4.10. □

It remains to add the last ingredient—groups of Lie type.

Theorem 4.12 *Let* F *be a perfect field. Then the automorphism group of the nonassociative simple Moufang loop* $M^*(F)$ *constructed over* F *is isomorphic to the semidirect product* $G_2(F) \rtimes \mathrm{Aut}(F)$*. Every automorphism of* $M^*(F)$ *is induced by a semilinear automorphism of the split octonion algebra* $\mathbb{O}F$*.*

Proof. We fix a perfect field F, and assume that all simple Moufang loops and Lie groups mentioned below are constructed over F.

The group with triality associated with M turns out to be its multiplication group $\mathrm{Mlt}(M) \cong D_4$, and the graph automorphisms of D_4 are exactly the triality automorphisms of M (cf. [27], [19]). To be more precise, Freudenthal proved this for the reals and Doro for finite fields, however they based their arguments only on the root system and parabolic subgroups, and that is why their result is valid over any field.

By [27], $C_{D_4}(\sigma) = B_3$, and by [38, Lemmas 4.9, 4.10 and 4.3], $C_{D_4}(\rho) = G_2$. As $G_2 < B_3$, by [31, p. 28], we have $C_{D_4}(S_3) = G_2$.

Since F is perfect, $\mathrm{Aut}(D_4)$ is isomorphic to $\Delta \rtimes (\mathrm{Aut}(F) \times S_3)$, by a result of Steinberg (cf. [9, Chapter 12]). Here, Δ is the group of the inner and diagonal automorphisms of D_4, and S_3 is the group of graph automorphisms of D_4. When $\mathrm{char}\, F = 2$ then no diagonal automorphisms exist, and $\Delta = \mathrm{Inn}(D_4)$. When $\mathrm{char}\, F \neq 2$ then S_3 acts faithfully on $\Delta/\mathrm{Inn}(D_4) \cong C_2 \times C_2$. Hence, in any case, $C_\Delta(S_3) = C_{D_4}(S_3)$. Moreover, for the field and graph automorphisms commute, we have $C_{\mathrm{Aut}(D_4)}(S_3) = C_{D_4}(S_3) \rtimes \mathrm{Aut}(F)$.

We have proved $\mathrm{Aut}(M) \cong G_2 \rtimes \mathrm{Aut}(F)$. The last statement follows from the fact that the group of linear automorphisms of the split octonion algebra is isomorphic to G_2. □

Corollary 4.13 $\mathrm{Aut}(M^*(q))$ *is a simple group if and only if* q *is an odd prime.*

Chapter 5

Small Moufang 2-loops

While working on the problem of Hamming distance of groups (see below), Drápal discovered two constructions that allowed him to begin a new approach to the classification of 2-groups (see [20], [21], [22], [23], [25]). In a joint paper [24] with the present author, the constructions were generalized to Moufang loops. It is now clear that the generalized constructions will be useful in the classification of Moufang 2-loops, too.

The classification of Moufang loops is finished for orders $n \leq 63$ (cf. [11], [29]). The methods used in [11] and [29] are very detailed, and several nontrivial constructions are required to account for all the loops.

We show in this chapter how to obtain all nonassociative Moufang loops of order 16 and 32, and how to construct thousands of Moufang loops of order 64. We hope to finish the classification of Moufang loops of order 64 in the near future, and add it to the electronic version of this thesis.

Proofs contained in [24] are omitted here. All machine calculation was done in GAP [28], and is briefly discussed in Section 5.5. For more on implementing loops and quasigroups in GAP, see Section 5.6.

5.1 Distances and modifications of Moufang loops

Let G be a set equipped with two binary operations $\cdot$, $*$ such that both $(G, \cdot)$, $(G, *)$ are loops. The *Hamming distance* $\mathrm{d}(\cdot, *)$ of $(G, \cdot)$ from $(G, *)$ is the cardinality of the set $\{(x, y) \in G \times G;\ x \cdot y \neq x * y\}$. The distance was studied extensively provided both $(G, \cdot)$, $(G, *)$ are groups (see the references above).

Instead of giving a vague description of the phenomenons, we collect some of the results here:

Theorem 5.1 *Let $(G, \cdot) \neq (G, *)$ be two groups of order n, and let $d = \mathrm{d}(\cdot, *)$. Then:*

(i) *$d \geq 6n - 24$ when $n \geq 51$,*

0	1	2	3
1	[2]	3	[0]
2	3	0	1
3	[0]	1	[2]

0	1	2	3
1	[0]	3	[2]
2	3	0	1
3	[2]	1	[0]

Figure 5.1: Quarter distance between C_4 and V_4.

(ii) *$d \geq 6n - 18$ when $n > 7$ is a prime,*

(iii) *if $d < n^2/9$ then the groups $(G, \cdot)$ and $(G, *)$ are isomorphic,*

(iv) *if n is a power of 2 and $d < n^2/4$ the groups $(G, \cdot)$ and $(G, *)$ are isomorphic.*

The proof of (i) and (iii) can be found in [20]. Part (ii) is proved in [54]. Finally, (iv) is from [21]. The results on which (i), (ii) are based are actually stronger in the sense that for any group $(G, \cdot)$ of order n with $n \geq 51$ or $n = p > 7$ it is known how far is the nearest group $(G, *)$ different from $(G, \cdot)$.

The bound $d < n^2/4$ in (iv) cannot be improved in general, as is documented by the distance of the cyclic group of order 4 from the Klein group, for instance. (See Figure 5.1.) The distance $n^2/4$ is an important value for 2-groups and Moufang 2-loops. It is known that if $(G, \cdot)$, $(G, *)$ are two groups of order 2^r, $r < 7$, or $(G, \cdot)$, $(G, *)$ are two Moufang loops of order 2^r, $r < 5$, then there are groups (resp. Moufang loops) $G_0 = (G, \cdot)$, G_1, ..., $G_m \cong (G, *)$ such that the distance between G_i and G_{i+1} is exactly $n^2/4$ (see [5], [24]). We now reveal how the intermediate Moufang loops G_1, ..., G_{m-1} are obtained.

5.1.1 Cyclic and dihedral modifications

Let $G = (G, \cdot)$ be a Moufang loop with a normal subloop S such that G/S is a cyclic group of order $2m$ or a dihedral group of order $4m$ (we count the 4-element Klein group among dihedral groups).

Given the set $M = \{1 - m, \ldots, m\}$, define the function $\sigma : \mathbb{Z} \longrightarrow \{-1, 0, 1\}$ by

$$\sigma(i) = \begin{cases} -1, & i < 1 - m, \\ 0, & i \in M, \\ 1, & i > m. \end{cases}$$

It is possible to deal with the cyclic and dihedral cases at the same time but, for the sake of clarity, let us discuss them separately, starting with the cyclic case.

Let α be a generator of G/S. We identify α with a subset of G. Then every $x \in G$ belongs to a unique coset α^i, where $i \in M$. Let h be some element of $Z(G) \cap S$. We are going to define a new multiplication $*$ on G: for $x \in \alpha^i$, $y \in \alpha^j$, let

$$x * y = xyh^{\sigma(i+j)}. \tag{5.1}$$

The resulting groupoid $(G, *)$ is called a *cyclic modification* of G with parameters G, S, h, α.

Now for the dihedral case. Let β, γ be two involutions of G/S such that $\alpha = \beta\gamma$ is a generator of the unique cyclic subgroup of order $2m$ in G/S. Let G_0 be the union of the cosets α^i, $i \in M$. Then G_0 is a subloop of index 2 in G. Set $G_1 = G \setminus G_0$. Pick $e \in \beta$, $f \in \gamma$ and $h \in N(G) \cap Z(G_0) \cap S$ such that $hxh = x$ for some (and hence all) $x \in G_1$. We are going to define a new multiplication $*$ on G. Note that every $x \in G$ belongs to a unique set $\alpha^i \cup e\alpha^i$, $i \in M$, and into unique set $\alpha^j \cup \alpha^j f$, $j \in M$. Assume that $x \in \alpha^i \cup e\alpha^i$ and $y \in (\alpha^j \cup \alpha^j f) \cap G_r$, where $r \in \{0, 1\}$. Then

$$x * y = xyh^{(-1)^r \sigma(i+j)}. \tag{5.2}$$

The resulting groupoid $(G, *)$ is called a *dihedral modification* of G with parameters G, S, h, β, γ. Note that the choice of $e \in \beta$, $f \in \gamma$ is of no influence on the multiplication $*$.

We now summarize some of the properties of the modifications (cf. [24]).

Theorem 5.2 *Let $G = (G, \cdot)$ be a Moufang loop of order n and let $(G, *)$ be its modification. Then:*

(i) *$(G, *)$ is a Moufang loop,*

(ii) *$\mathrm{d}(\cdot, *) = n^2/4$,*

(iii) *$N(G, \cdot) = N(G, *)$ as a set,*

(iv) *$A(G, \cdot) = A(G, *)$ as a subloop,*

(v) *the associators (as maps from $G \times G \times G$ to $A(G)$) are equivalent.*

An important observation is that the centers of $(G, \cdot)$ and $(G, *)$ are not necessarily the same (or even of the same size) and hence $(G, \cdot)$ is not necessarily isomorphic to $(G, *)$.

Let $(G, \cdot)$, $(G, *)$ be two Moufang loops of the same order. We say that they are *connected* if there are Moufang loops $G_0 = (G, \cdot)$, G_1, $\ldots$, $G_m \cong (G, *)$ such that G_{i+1} is a modification of G_i. By Theorem 5.2(v), the Moufang loops can only be connected if their associators are equivalent. The question is whether the converse is true, at least for Moufang 2-loops.

The answer is negative, as it is known that one cannot connect all groups of order 64 by the modifications (cf. [5]). Nevertheless, any two Moufang loops of order at most 32 that have equivalent associator are connected, as we are going to show next.

5.2 Notation

Let $(G, \cdot) = \{1, \ldots, n\}$ be a group of order n. Recall the loops $M(G, 2)$ from Chapter 3. When $M = (m_{ij})_{n \times n}$ is a multiplication table of G with $m_{ij} = g_i \cdot g_j$, let us agree

that the canonical multiplication table of $M(G,2)$ will be $L = (l_{ij})_{2n\times 2n}$, where

$$l_{ij} = \begin{cases} g_i \cdot g_j, & 1 \le i,\, j \le n, \\ (g_{j-n} \cdot g_i) + n, & 1 \le i \le n,\, n < j \le 2n, \\ (g_{i-n} \cdot g_j^{-1}) + n, & n < i \le 2n,\, 1 \le j \le n, \\ (g_{j-n}^{-1} \cdot g_{i-n}) + n, & n < i,\, j \le 2n. \end{cases} \tag{5.3}$$

When G, S, h, α are parameters of a cyclic modification, we will describe the resulting Moufang loop $(G,*)$ as

`CM( G, Elements( S ), h, a )`,

where `Elements( S )` is a list of elements of S, and `a` is any element of the coset α.

Similarly, when G, S, h, β, γ are parameters of a dihedral modification, we will describe the resulting Moufang loop $(G,*)$ as

`DM( G, Elements( S ), h, e, f )`,

where `e` is some element of β, and `f` is some element of γ.

The multiplication formulae (5.1), (5.2), and (5.3) can then be used to obtain a uniquely determined multiplication table for $(G,*)$.

5.3 Moufang loops of order 16 and 32

Up to isomorphism, there are 5 nonassociative Moufang loops of order 16, and 71 nonassociative Moufang loops of order 32, according to [29]. All these loops (resp. their multiplication tables) are listed in [29]. The kth nonassociative Moufang loop of order n is denoted by n/k. Using the modifications introduced in Subsection 5.1.1, we give a much more compact description of all nonassociative Moufang loops of order 16 and 32. Unfortunately, at this point, the fact that the classification is complete follows from [11] and [29]—not from our theory.

Here is how all 5 nonassociative Moufang loops of order 16 are found. Table 5.3 gives a multiplication table for the dihedral group D_4 of order 8. Table 5.2 then shows how all 5 nonassociative Moufang loops of order 16 are obtained by modifications. It uses the notational conventions of Section 5.2.

Let us now describe all 71 nonassociative Moufang loops of order 32. Not all such loops have an equivalent associator. This is seen quickly from the fact that some of them have nucleus of size 4, for instance 32/1, while others have nucleus of size 2, for instance 32/7. As it turns out, all other nonassociative Moufang loops of order 32 can be obtained as modifications of 32/1 and 32/7. The loop 32/1 is $M(D_4 \times C_2, 2)$ and the loop 32/7 is $M(D_8, 2)$. The multiplication tables of $D_4 \times C_2$ and D_8 we used are in Tables 5.3 and 5.4, respectively. Tables 5.5 and 5.6 then show how the modifications yield all nonassociative Moufang loops of order 32.

Table 5.1: Multipication table of D_4

	1	2	3	4	5	6	7	8
1	1	2	3	4	5	6	7	8
2	2	3	4	1	6	7	8	5
3	3	4	1	2	7	8	5	6
4	4	1	2	3	8	5	6	7
5	5	8	7	6	1	4	3	2
6	6	5	8	7	2	1	4	3
7	7	6	5	8	3	2	1	4
8	8	7	6	5	4	3	2	1

Table 5.2: Nonassociative Moufang loops of order 16

16/1 = M(D_4, 2),
16/2 = DM(16/1, [1, 2, 3, 4], 5, 9, 3),
16/4 = CM(16/1, [1, 3, 5, 7, 9, 11, 13, 15], 2, 3),
16/5 = CM(16/1, [1, 2, 3, 4, 5, 6, 7, 8], 9, 3),
16/3 = DM(16/5, [1, 2, 3, 4], 13, 9, 3).

Table 5.3: Multiplication table of $D_4 \times C_2$

	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
1	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
2	2	3	4	1	6	7	8	5	10	11	12	9	14	15	16	13
3	3	4	1	2	7	8	5	6	11	12	9	10	15	16	13	14
4	4	1	2	3	8	5	6	7	12	9	10	11	16	13	14	15
5	5	8	7	6	1	4	3	2	13	16	15	14	9	12	11	10
6	6	5	8	7	2	1	4	3	14	13	16	15	10	9	12	11
7	7	6	5	8	3	2	1	4	15	14	13	16	11	10	9	12
8	8	7	6	5	4	3	2	1	16	15	14	13	12	11	10	9
9	9	10	11	12	13	14	15	16	1	2	3	4	5	6	7	8
10	10	11	12	9	14	15	16	13	2	3	4	1	6	7	8	5
11	11	12	9	10	15	16	13	14	3	4	1	2	7	8	5	6
12	12	9	10	11	16	13	14	15	4	1	2	3	8	5	6	7
13	13	16	15	14	9	12	11	10	5	8	7	6	1	4	3	2
14	14	13	16	15	10	9	12	11	6	5	8	7	2	1	4	3
15	15	14	13	16	11	10	9	12	7	6	5	8	3	2	1	4
16	16	15	14	13	12	11	10	9	8	7	6	5	4	3	2	1

Table 5.4: Multiplication table of D_8

	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
1	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
2	2	3	4	5	6	7	8	1	10	11	12	13	14	15	16	9
3	3	4	5	6	7	8	1	2	11	12	13	14	15	16	9	10
4	4	5	6	7	8	1	2	3	12	13	14	15	16	9	10	11
5	5	6	7	8	1	2	3	4	13	14	15	16	9	10	11	12
6	6	7	8	1	2	3	4	5	14	15	16	9	10	11	12	13
7	7	8	1	2	3	4	5	6	15	16	9	10	11	12	13	14
8	8	1	2	3	4	5	6	7	16	9	10	11	12	13	14	15
9	9	16	15	14	13	12	11	10	1	8	7	6	5	4	3	2
10	10	9	16	15	14	13	12	11	2	1	8	7	6	5	4	3
11	11	10	9	16	15	14	13	12	3	2	1	8	7	6	5	4
12	12	11	10	9	16	15	14	13	4	3	2	1	8	7	6	5
13	13	12	11	10	9	16	15	14	5	4	3	2	1	8	7	6
14	14	13	12	11	10	9	16	15	6	5	4	3	2	1	8	7
15	15	14	13	12	11	10	9	16	7	6	5	4	3	2	1	8
16	16	15	14	13	12	11	10	9	8	7	6	5	4	3	2	1

Table 5.5: Moufang loops of order 32; component of 32/1

32/1	=	M($D_4 \times C_2$, 2)
32/12	=	DM(32/1, [1, 3, 13, 15, 21, 23, 25, 27], 6, 5, 3)
32/11	=	CM(32/1, [1, 3, 5, 7, 9, 11, 13, 15, 17, 19, 21, 23, 25, 27, 29, 31], 2, 3)
32/3	=	DM(32/1, [1, 3, 10, 12, 21, 23, 30, 32], 6, 5, 3)
32/10	=	CM(32/1, [1, 3, 5, 7, 10, 12, 14, 16, 17, 19, 21, 23, 26, 28, 30, 32], 2, 3)
32/18	=	DM(32/1, [1, 3, 10, 12, 21, 23, 30, 32], 2, 5, 3)
32/22	=	DM(32/1, [1, 3, 14, 16, 21, 23, 26, 28], 2, 5, 3)
32/19	=	CM(32/1, [1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16], 17, 3)
32/60	=	CM(32/1, [1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16], 17, 9)
32/2	=	DM(32/1, [1, 2, 3, 4, 9, 10, 11, 12], 5, 17, 3)
32/5	=	DM(32/1, [1, 2, 3, 4, 9, 10, 11, 12], 5, 17, 9)
32/69	=	DM(32/1, [1, 3, 5, 7, 9, 11, 13, 15], 2, 17, 11)
32/70	=	CM(32/1, [1, 3, 5, 7, 9, 11, 13, 15, 17, 19, 21, 23, 25, 27, 29, 31], 2, 11)
32/4	=	DM(32/1, [1, 3, 5, 7, 9, 11, 13, 15], 18, 17, 11)
32/17	=	CM(32/12, [1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16], 17, 3)
32/13	=	CM(32/12, [1, 2, 3, 4, 13, 14, 15, 16, 21, 22, 23, 24, 25, 26, 27, 28], 5, 3
32/14	=	DM(32/12, [1, 3, 14, 16, 21, 23, 26, 28], 2, 5, 3)
32/41	=	CM(32/11, [1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16], 17, 9)
32/50	=	DM(32/11, [1, 2, 3, 4, 9, 10, 11, 12], 5, 17, 9)
32/57	=	DM(32/11, [1, 3, 5, 7, 9, 11, 13, 15], 2, 18, 11)
32/48	=	DM(32/11, [1, 3, 6, 8, 9, 11, 14, 16], 2, 17, 11)
32/68	=	DM(32/11, [1, 3, 5, 7, 9, 11, 13, 15], 18, 17, 9)
32/40	=	CM(32/11, [1, 3, 5, 7, 9, 11, 13, 15, 18, 20, 22, 24, 26, 28, 30, 32], 2, 9)
32/55	=	DM(32/11, [1, 3, 9, 11, 22, 24, 30, 32], 6, 5, 9)
32/6	=	DM(32/3, [1, 2, 3, 4, 9, 10, 11, 12], 5, 17, 11)
32/15	=	CM(32/3, [1, 2, 3, 4, 9, 10, 11, 12, 21, 22, 23, 24, 29, 30, 31, 32], 5, 3)
32/21	=	DM(32/3, [1, 3, 10, 12, 22, 24, 29, 31], 2, 5, 3)
32/20	=	CM(32/3, [1, 3, 5, 7, 10, 12, 14, 16, 18, 20, 22, 24, 25, 27, 29, 31], 2, 3)
32/24	=	CM(32/10, [1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16], 17, 9)
32/23	=	CM(32/10, [1, 3, 5, 7, 9, 11, 13, 15, 17, 19, 21, 23, 25, 27, 29, 31], 2, 9)
32/26	=	DM(32/22, [1, 3, 6, 8, 9, 11, 14, 16], 2, 17, 9)
32/67	=	DM(32/19, [1, 2, 3, 4, 9, 10, 11, 12], 5, 17, 9)
32/16	=	DM(32/19, [1, 2, 3, 4, 9, 10, 11, 12], 21, 17, 3)
32/39	=	CM(32/19, [1, 2, 3, 4, 9, 10, 11, 12, 17, 18, 19, 20, 25, 26, 27, 28], 5, 9)
32/56	=	DM(32/19, [1, 2, 3, 4, 9, 10, 11, 12], 21, 17, 9)
32/47	=	DM(32/19, [1, 3, 9, 11, 17, 19, 25, 27], 2, 5, 11)
32/51	=	DM(32/19, [1, 3, 5, 7, 9, 11, 13, 15], 18, 17, 11)
32/54	=	DM(32/60, [1, 2, 3, 4, 9, 10, 11, 12], 5, 17, 3)
32/65	=	DM(32/60, [1, 2, 3, 4, 9, 10, 11, 12], 21, 17, 3)
32/62	=	DM(32/60, [1, 2, 3, 4, 9, 10, 11, 12], 21, 17, 9)
32/53	=	DM(32/60, [1, 2, 3, 4, 9, 10, 11, 12], 21, 17, 11)
32/46	=	DM(32/60, [1, 3, 9, 11, 17, 19, 25, 27], 2, 5, 11)
32/61	=	DM(32/60, [1, 3, 9, 11, 17, 19, 25, 27], 2, 5, 9)
32/63	=	DM(32/60, [1, 3, 5, 7, 9, 11, 13, 15], 18, 17, 11)
32/64	=	DM(32/60, [1, 3, 9, 11, 17, 19, 25, 27], 6, 5, 9)
32/52	=	DM(32/5, [1, 3, 9, 11, 21, 23, 29, 31], 2, 5, 11)
32/71	=	DM(32/5, [1, 3, 5, 7, 9, 11, 13, 15], 18, 17, 11)
32/45	=	DM(32/69, [1, 3, 9, 11, 22, 24, 30, 32], 2, 5, 9)
32/59	=	CM(32/69, [1, 3, 5, 7, 9, 11, 13, 15, 18, 20, 22, 24, 26, 28, 30, 32], 2, 9)
32/25	=	DM(32/13, [1, 3, 5, 7, 9, 11, 13, 15], 2, 18, 9)
32/30	=	DM(32/14, [1, 2, 3, 4, 9, 10, 11, 12], 5, 17, 11)
32/29	=	DM(32/14, [1, 3, 9, 11, 21, 23, 29, 31], 6, 5, 9)
32/66	=	DM(32/41, [1, 2, 3, 4, 9, 10, 11, 12], 21, 17, 9)
32/43	=	DM(32/41, [1, 3, 9, 11, 17, 19, 25, 27], 2, 6, 11)
32/42	=	DM(32/41, [1, 3, 6, 8, 9, 11, 14, 16], 18, 17, 9)
32/49	=	DM(32/50, [1, 3, 9, 11, 21, 23, 29, 31], 2, 6, 11)
32/58	=	CM(32/50, [1, 3, 6, 8, 9, 11, 14, 16, 18, 20, 21, 23, 26, 28, 29, 31], 2, 9)
32/44	=	DM(32/57, [1, 3, 6, 8, 9, 11, 14, 16], 18, 17, 9)
32/36	=	CM(32/6, [1, 2, 3, 4, 9, 10, 11, 12, 21, 22, 23, 24, 29, 30, 31, 32], 5, 3)
32/35	=	CM(32/21, [1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16], 17, 11)

Table 5.6: Moufang loops of order 32; component of 32/7

32/7	=	M(D8, 2)
32/31	=	DM(32/7, [1, 3, 5, 7, 25, 27, 29, 31], 2, 9, 5)
32/37	=	DM(32/7, [1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16], 17, 5)
32/9	=	DM(32/7, [1, 2, 3, 4, 5, 6, 7, 8], 9, 17, 5)
32/8	=	DM(32/7, [1, 3, 5, 7, 25, 27, 29, 31], 10, 9, 5)
32/27	=	DM(32/7, [1, 3, 5, 7, 9, 11, 13, 15, 17, 19, 21, 23, 25, 27, 29, 31], 2, 5)
32/32	=	DM(32/31, [1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16], 17, 5)
32/33	=	DM(32/31, [1, 3, 5, 7, 9, 11, 13, 15, 18, 20, 22, 24, 26, 28, 30, 32], 2, 5)
32/28	=	DM(32/31, [1, 3, 5, 7, 26, 28, 30, 32], 10, 9, 5)
32/34	=	DM(32/31, [1, 3, 5, 7, 10, 12, 14, 16, 18, 20, 22, 24, 25, 27, 29, 31], 2, 5)
32/38	=	DM(32/37, [1, 2, 3, 4, 5, 6, 7, 8], 25, 17, 5)

5.4 Constructing Moufang loops of order 64

Following the strategy for $n = 16$ and 32, we set out to construct Moufang loops of order 64 as modifications of the loops $M(G, 2)$, where G is a nonabelian group of order 32.

There are 44 nonabelian groups of order 32. Let M_1, ..., M_{44} be the corresponding loops $M(G, 2)$. Just by looking at the cardinality of the nucleus and the isomorphism type of the associator subloop of the loops M_i, we find out that there are at least 7 components of connectivity among nonassociative Moufang loops of order 64.

At the time of writing of this thesis, the GAP calculations were still in progress, attempting to find all modifications of the loops M_i. More than 3500 pairwise nonisomorphic nonassociative Moufang loops of order 64 were found already. More precise results will be added to the electronic version of this thesis once the calculation is complete.

The most expensive part of the calculation is the determination of the isomorphism type of the produced modifications.

5.5 How GAP was used

The results of this chapter rely heavily on computation in GAP. We used a GAP package LOOPS [39], that is being developed by G. P. Nagy and the author. See next section for more on [39].

Here is a brief outline of the algorithm that was used to construct all modifications of a Moufang loop M. Typically, M is of the form $M(G, 2)$, where G is a nonabelian group of order 2^{r-1}, but it is not necessary to assume this.

In every step, all one-step modifications of a given loop are found, by exhausting all possible parameters for modifications. These newly found modifications are then compared to all loops obtained earlier. If a loop is found that is not isomorphic to any of the previously generated loops, it is stored in a tree as a child of the loop it was obtained from. For instance, the complete tree for $r = 4$ (i.e., $n = 16$) is

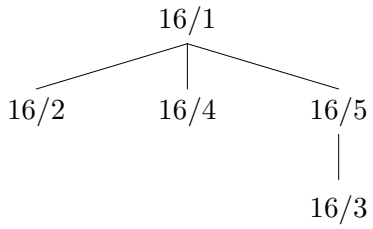

Figure 5.2: All nonassociative Moufang loops of order 16 constructed by modifications.

depicted in Figure 5.2, as can be seen from Table 5.2.

As we have already noted, the bottleneck of the algorithm is the test for isomorphism between the newly obtained modifications and the loops in the tree. We offer a few empirical remarks on this topic.

Given two groups (of the same order), one can test if they are isomorphic relatively quickly by constructing a canonical presentation for each of the groups. Since the theory of presentations for Moufang loops is not well understood, we used a different strategy.

For each Moufang 2-loop L we construct the *discriminator* $D(L) = (I(L), P(L))$, where $I(L)$ is a list of invariants of L under isomorphism, and $P(L) = (P(L)[1], \ldots, P(L)[t])$ is a partition of the elements of L such that: if M is isomorphic to L and $\varphi : L \longrightarrow M$ is an isomorphism then $\varphi(P(L)[i]) = P(M)[i]$.

The idea is to come up with properties that can be computed cheaply yet produce a fine partition $P(L)$. Without going into details, it turns out that a good property for Moufang 2-loops is the cardinality of the centralizer of a given element. Several additional properties "quadratic in complexity" were actually used.

If L, M are two loops and $D(L)$, $D(M)$ are already calculated, the algorithm attempts to construct a bijection $L \longrightarrow M$ preserving the partitions $P(L)$, $P(M)$, so that it is a homomorphism.

5.6 Loops and quasigroups in GAP

This short section describes the GAP package LOOPS [39] that is currently being developed by G. P. Nagy and the author. We hope that the package will eventually become a standard tool for loop theorists. Our intention is not to give a detailed description of the syntax here, but to convey the main idea of the package instead.

In order to perform calculations in groups quickly, one usually uses a permutation representation. Due to the lack of associativity, no such simple representation is possible for loops (but see [47]). In the end, one probably has to resort to multiplication tables in most cases. However, this does not mean that all calculation should be performed on the level of multiplication tables. On the contrary, whenever possible,

the algorithms should be based on permutation groups associated with loops. Let us illustrate this approach with a few examples.

Let Q be a quasigroup defined by a multiplication table, and let S be a subset of Q. We want to find the smallest subquasigroup of Q containing S. This can be done directly (and slowly in GAP) by working with the multiplication table, or the problem can be translated into permutation groups as follows: let T be the set consisting of all left and right translations of Q by elements of S. Let G be the permutation group generated by T, and let $O(s)$ be the orbit of $s \in S$ under G. Then the subquasigroup we are looking for is the union of the orbits $O(s)$, for $s \in S$. The corresponding simplified code in GAP looks as follows:

```
T := Set([]);   #empty set
for s in S do
    AddSet( T, LeftSection( Q )[ s ] );
    AddSet( T, RightSection( Q )[ s ] );
od;
return Union( Orbits( Group( T ), S ) );
```

The only two functions in this code not included in the standard libraries of GAP are `LeftSection` and `RightSection`. Of course, these two sections must be initially obtained from the multiplication table of Q, however, this is the only time the multiplication table of Q is needed. Thus `LeftSection` and `RightSection` are good examples of data that should be stored as attributes of Q once they are calculated.

Here is a simplified code for the left nucleus of Q:

```
L := LeftSection( Q );
return Filtered( Q,
    x -> ForAll( Q, y -> L[ y ]*L[ x ] = L[ x*y ] )
);
```

This surely deserves some explanation. By definition, an element $x \in Q$ belongs to $N_\lambda(Q)$ if and only if $x(yz) = (xy)z$ holds for every y, $z \in Q$. In terms of left translations, $zL_yL_x = zL_{xy}$ must hold for every y, $z \in Q$. Thus there is no need to refer to z; we merely have to check that $L_yL_x = L_{xy}$ for every $y \in Q$. The above code accomplishes just that.

Finally, let us test whether a subloop S is normal in a loop L. It suffices to show that S is closed under all inner mappings of L, in fact, under some generators of the inner mapping group of Q. First, we calculate the multiplication group of L:

```
Group( Union( LeftSection( L ), RightSection( L ) ) );
```

Recall that the inner mapping group consists of all elements of the multiplication group that fix the neutral element. In GAP:

```
Stabilizer( MultiplicationGroup( L ), One( L ) );
```

Finally, here is a function that tests whether S is normal in L:

```
return ForAll( GeneratorsOfGroup( InnerMappingGroup( L ) ),
    g -> S = OnSets( S, g )
);
```

This should suffice as an illustration of our approach. See [39] for more details.

Bibliography

[1] A. A. Albert, J. Thompson, *Two-element generation of the projective unimodular group*, Illinois J. Math. **3** (1959), 421–439.

[2] M. Aschbacher, Sporadic groups, Cambridge Tracts in Mathematics **104**. Cambridge University Press, Cambridge, 1994.

[3] M. Aschbacher, R. Guralnick, *Some applications of the first cohomology group*, J. Algebra **90** (1984), no. 2, 446–460.

[4] R. Baer, *Nets and groups*, Trans. Amer. Math. Soc. **46** (1939), 110–141.

[5] M. Bálek, A. Drápal, and N. Zhukavets, *The neighbourhood of dihedral* 2*-groups*, submitted.

[6] E. Bannai, S. Song, *The character tables of Paige's simple Moufang loops and their relationship to the character tables of* $\mathrm{PSL}(2, q)$, Proc. London Math. Soc. (3) **58** (1989), no. 2, 209–236.

[7] A. Barlotti, K. Strambach, *The geometry of binary systems*, Advances Math. **49** (1983), 1–105.

[8] R. H. Bruck, A survey of binary systems. Springer-Verlag, Berlin, 1958.

[9] R. W. Carter, Simple groups of Lie type. Wiley Interscience, 1972.

[10] O. Chein, *Moufang Loops of Small Order I*, Trans. Amer. Math. Soc. **188** (1974), 31–51.

[11] O. Chein, *Moufang loops of small order*, Memoirs of the American Mathematical Society, Volume **13**, Issue 1, Number **197** (1978).

[12] O. Chein, E. Goodaire, *Moufang loops with a unique nonidentity commutator (associator, square)*, J. Algebra **130** (1990), 369–384.

[13] O. Chein, M. Kinyon, A. Rajah, P. Vojtěchovský, *Loops and the Lagrange property*, to appear in Results in Mathematics.

[14] O. Chein, H. O. Pflugfelder, *The smallest Moufang loop*, Arch. Math. **22** (1971), 573–576.

[15] O. Chein, H. O. Pflugfelder, J. D. H. Smith (eds.), Quasigroups and Loops: Theory and Applications, *Sigma series in pure mathematics* **8**, Heldermann Verlag Berlin, 1990.

[16] H. S. M. Coxeter, *Integral Cayley Numbers*, Duke Mathematical Journal, Vol. 13, No. 4, December, 1946. Reprinted in H. S. M. Coxeter, *Twelve Geometric Essays*, Southern Illinois University Press, 1968.

[17] H. S. M. Coxeter, W. O. J. Moser, *Generators and relations for discrete groups.* Fourth edition. Ergebnisse der Mathematik und ihrer Grenzgebiete [Results in Mathematics and Related Areas], **14**. Springer-Verlag, Berlin-New York (1980).

[18] L. E. Dickson, *Linear Groups with an Exposition of the Galois Field Theory*, Teubner (1901); reprinted by Dover (1958).

[19] S. Doro, *Simple Moufang loop*, Math. Proc. Cambridge Philos. Soc. **83** (1978), 377–392.

[20] A. Drápal, *How fart appart can the group multiplication tables be?*, Europ. J. of Combin. **13**(1992), 335–343.

[21] A. Drápal, *Non-isomorphic* 2*-groups coincide at most in three quarters of their multiplication tables*, European J. Combin. **21** (2000), 301–321.

[22] A. Drápal, *On groups that differ in one of four squares*, European J. Combin. **23** (2002), 899–918.

[23] A. Drápal, *Cyclic and dihedral constructions of even order*, submitted.

[24] A. Drápal, P. Vojtěchovský, *Moufang loops that share associator and three quarters of their multiplication tables*, submitted.

[25] A. Drápal, N. Zhukavets, *On multiplication tables of groups that agree on half of columns and half of rows*, to appear in Glasgow Mathematical Journal.

[26] N. J. Fine, *Binomial coefficients modulo a prime*, Mathematical Association of America Monthly **54**(1947), 589–592.

[27] H. Freudenthal, *Oktaven, Ausnahmegruppen und Oktavengeometrie*, Geometria Dedicata **19** (1985), 1–63.

[28] The GAP Group, GAP — Groups, Algorithms, and Programming, Version 4.3; Aachen, St Andrews (1999). (Visit http://www-gap.dcs.st-and.ac.uk/~gap).

[29] E. G. Goodaire, S. May, M. Raman, The Moufang Loops of Order less than 64, Nova Science Publishers, 1999.

[30] D. Gorenstein, Finite groups. Second edition. Chelsea Publishing Co., New York (1980).

[31] D. Gorenstein, R. Lyons, R. Solomon, The classification of the finite simple groups, No. 3. Part I, Mathematical Surveys and Monographs **40**(3) (Providence, R.I., AMS, 1998).

[32] R. L. Griess, Jr., *Code Loops*, J. Algebra **100** (1986), 224–234.

[33] J. I. Hall, G. P. Nagy, *On Moufang 3-nets and groups with triality*, Acta Sci. Math. (Szeged) **67** (2001), 675–685.

[34] D. R. Hankerson, D. G. Hoffman, D. A. Leonard, C. C. Lindner, K. T. Phelps, C. A. Rodger, J. R. Wall, Coding theory and cryptography: The essentials. Second edition, revised and expanded. Marcel Dekker, New York, 2000.

[35] T. Hsu, *Moufang loops of class* 2 *and cubic forms*, Math. Proc. Cambridge Philos. Soc. **128** (2000), no. 2, 197–222.

[36] T. Hsu, *Explicit constructions of code loops as centrally twisted products*, Math. Proc. Cambridge Philos. Soc. **128** (2000), no. 2, 223–232.

[37] K. W. Johnson, P. Vojtěchovský, *Dedekind quasigroups*, in preparation.

[38] M. W. Liebeck, *The classification of finite simple Moufang loops*, Math. Proc. Cambridge Philos. Soc. **102** (1987), 33–47.

[39] LOOPS, a package for GAP for calculations with quasigroups and loops. By G. P. Nagy and P. Vojtěchovský. Under preparation. The project's webpage is http://www.math.du.edu/loops/loops.html

[40] Mathematica 4.1, Wolfram Research, 2003.

[41] P. T. Nagy, K. Strambach, *Loops as invariant sections in groups, and their geometry*, Canad. J. Math. **46** (1994), no. 5, 1027–1056.

[42] G. P. Nagy, P. Vojtěchovský, *Automorphism groups of simple Moufang loops over perfect fields*, Math. Proc. Cambridge Philos. Soc., to appear.

[43] G. P. Nagy, P. Vojtěchovský, *Octonions, simple Moufang loops and triality*, to appear in Quasigroups and Related Systems, proceedings of Workshops Loops '03.

[44] L. J. Paige, *A class of simple Moufang loops*, Proc. Amer. Math. Soc. **7** (1956), 471–482.

[45] H. O. Pflugfelder, Quasigroups and Loops: Introduction, *Sigma series in pure mathematics* **7**, Heldermann Verlag Berlin, 1990.

[46] T. M. Richardson, *Local subgroups of the Monster and odd code loops*, Trans. Amer. Math. Soc. **347** (1995), no. 5, 1453–1531.

[47] J. D. H. Smith, *Quasigroup actions: Markov chains, pseudoinverses, and linear representations*, Southeast Asian Bull. Math. **23** (1999), no. 4, 719–729.

[48] J. D. H. Smith, *A left loop on the* 15*-sphere*, J. Algebra **176** (1995), no. 1, 128–138.

[49] T. A. Springer, F. D. Veldkamp, Octonions, Jordan Algebras, and Exceptional Groups. Springer Monographs in Mathematics (Springer Verlag, 2000).

[50] J. H. van Lint, Introduction to coding theory. Third edition. Graduate texts in mathematics **86**, Springer-Verlag, Berlin, 1999.

[51] J. H. van Lint, R. M. Wilson, A Course in Combinatorics. Cambridge University Press, Cambridge, 1992.

[52] P. Vojtěchovský, *Combinatorial aspects of code loops*, Comment. Math. Univ. Carolinae **41, 2** (2000), 429–435.

[53] P. Vojtěchovský, *Combinatorial polarization, code loops and codes of high level*, submitted to International Journal of Mathematics and Mathematical Sciences, proceedings of CombinaTexas 2003 comference.

[54] P. Vojtěchovský, *Distances of groups of prime order*, Contributions to General Algebra **11**, Proceedings of the Olomouc Workhop '98, I. Chajda et al. (eds.), Verlag Johannes Heyn, Klagenfurt, 1999.

[55] P. Vojtěchovský, Finite simple Moufang loops. PhD Thesis, Iowa State University, 2001.

[56] P. Vojtěchovský, *Generators for finite simple Moufang loops*, J. of Group Theory **6** (2003), 169–174.

[57] P. Vojtěchovský, *Generators of Nonassociative Simple Moufang Loops over Finite Prime Fields*, J. of Algebra **241** (2001), 186–192.

[58] P. Vojtěchovský, *Investigation of subalgebra lattices by means of Hasse constants*, to appear in Algebra Universalis.

[59] P. Vojtěchovský, *On the uniqueness of loops* $M(G, 2)$, Comment. Math. Univ. Carolinae, to appear.

[60] P. Vojtěchovský, *Random generators of given orders and the smallest simple Moufang loop*, to appear in Algebra Universalis.

[61] P. Vojtěchovský, *The smallest Moufang loop revisited*, to appear in Results in Mathematics.

[62] H. N. Ward, *Combinatorial Polarization*, Discrete Mathematics **26**(1979), 185–197.

Index