MATEMATICKO-FYZIKÁLNÍ FAKULTA
UNIVERZITA KARLOVA

Katedra algebry

SOUVISLOSTI KÓDŮ, GRUP A LUP

Autoreferát doktorské disertační práce

Petr Vojtěchovský

Školitel: doc. Aleš Drápal, CSc.

Obor M2-Algebra

PRAHA 2003

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

Dizertační práce vznikla v rámci externího doktorandského studia na MFF UK v letech 1998–2002.

Uchazeč:

Mgr. Petr Vojtěchovský
Katedra algebry MFF UK
Sokolovská 83
186 75 Praha 8

Školitel:

doc. RNDr. Aleš Drápal, CSc.
Katedra algebry MFF UK
Sokolovská 83
186 75 Praha 8

Školící pracoviště:

Katedra algebry MFF UK
Sokolovská 83
186 75 Praha 8

Oponenti:

Autoreferát byl odeslán dne: ....

Obhajoba disertační práce se koná dne .... v .... hod. před komisí obhajoby doktorských disertačních prací v oboru M2 na MFF UK, Ke Karlovu 3, Praha 2, v místnosti č. ....

S disertací je možno se seznámit na Útvaru doktorandského studia MFF UK, Ke Karlovu 3, Praha 2.

Předsedou oborové rady oboru M2 je RNDr. Jaroslav Ježek, DrSc., Katedra algebry MFF UK, Sokolovská 83, 186 75 Praha 8.

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 [4], [9], [14], [17], [18], [20], [21], [22], [23], [24], [25], [26], [27], [28], [29].

Each chapter can be read independently once the reader becomes familiar with the notation and terminology, nevertheless some effort was made to present the entire work in a uniform way.

It was our intention to avoid most of the results that appeared already in [23]—the doctoral thesis written under the supervision of Jonathan D. H. Smith at Iowa State University. Nevertheless some overlap exists.

Here is the summary of results:

1. Combinatorial Polarization

Combinatorial polarization is a process similar to the principle of inclusion and exclusion. When V is a vector space over F and $f : V \longrightarrow F$ is an arbitrary map, the sth derived form of f is the map $\delta_s f : V^s \longrightarrow F$ defined by

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

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. We prove:

Theorem 1.1. *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 $\mathbf{x} = (x_1, \dots, x_n)$, $\mathbf{a} = (a_1, \dots, a_n)$, 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

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

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

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

We then develop a counting technique (based on the number of partitions of an integer into a sum of integers of restricted size) that allows us to determine the dimension of the vector space consisting of all maps $V \longrightarrow F$ whose combinatorial degree is at most d.

Combinatorial polarization is used while dealing with code loops (see below). A binary linear code is said to be of level r is 2^r divides the Hamming weight $w(c)$ of every codeword c, and if r is as big as possible. Codes of level 2 are also called doubly even.

Code loops were originally defined by Griess [13] as follows: Let C be a doubly even code over $F = \{0, 1\}$. Let $\eta : C \times C \longrightarrow F$ be a map satisfying

$$\begin{aligned}
&\eta(x, x) = w(x)/4,\\
&\eta(x, y) + \eta(y, x) = w(x \cap y)/2,\\
&\eta(x, y) + \eta(x + y, z) + \eta(y, z) + \eta(x, y + z) = w(x \cap y \cap z),
\end{aligned}$$

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

$$(x, a)(y, b) = (x + y, a + b + \eta(x, y))$$

is a code loop.

Every code loop is Moufang, i.e., it satisfies the identity $x(y(xz)) = ((xy)x)z$. After discussing extensions of abelian groups by (Moufang) loops, we recall how Chein and Goodaire [3] proved that code loops are exactly finite Moufang loops with at most two squares. One of the crucial steps in their proof is a construction of a doubly even code with prescribed weights of intersections. We generalize and simplify their construction as follows:

Theorem 1.2. *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 $c \in C$.*

Finally, we calculate the polynomial map of combinatorial degree 3 associated with the extended binary Golay code, and point out that some of its monomials form a 2-$(11, 3, 3)$ design.

2. Moufang Loops with a Subgroup of Index Two

Following Chein [2], let G be a group of order n and let $\overline{G} = \{\overline{x};\ x \in G\}$ be a set of new elements. Define multiplication $*$ on $G \cup \overline{G}$ by

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

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

We first demonstrate that many Moufang loops are of the type $M(G, 2)$. Then we show that the above construction is essentially unique:

Theorem 2.1. *Let G with $|G| > 1$ be a finite group that is not an elementary abelian 2-group. Assume that*

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

specifies the multiplication in the four quarters of $L = G \cup \overline{G}$, 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 Bol (i.e., it satisfies the identity $x(y(xz)) = (x(yx))z$), then it is Moufang.

Moreover, 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.

We then move on to derive presentations for loops $M(G, 2)$ when G is a 2-generated group:

Theorem 2.2. *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*

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

where 1 is the neutral element of G.

Guided by this presentation, we discover a neat visual description of the smallest 12-element nonassociative Moufang loop $M(S_3, 2)$.

3. 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. These Paige loops [19] are constructed as follows. Let F be any field. Then the split octonion algebra $\mathbb{O}(F)$ consist of all vector matrices

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

where a, $b \in F$ and α, $\beta \in F^3$. The addition is performed component-wise, and the multiplication is governed by

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

where $\cdot$ is the usual dot product, and $\times$ is the usual vector product. The norm on $\mathbb{O}(F)$ is the determinant $\det x = ab - \alpha\cdot\beta$. Then the set $M(F) = \{x \in \mathbb{O}F;\ \det x = 1\}$ is closed under multiplication and is a Moufang loop. Moreover, $M^*(F) = M(F)/Z(M(F))$ is simple for any field F. It is well-known that there are no other nonassociative finite simple Moufang loops besides the finite Paige loops constructed above [15].

No nonassociative Moufang loop is two-generated. After studying the generators of special linear and unimodular groups, we show:

Theorem 3.1. *Every nonassociative finite simple Moufang loop is 3-generated.*

We then focus on automorphism groups of Paige loops over perfect fields, and prove (with G. P. Nagy):

Theorem 3.2. *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 $\mathbb{O}(F)$.*

Here, $G_2(F)$ is the Chevalley group of type G_2. The above result is proved using geometrical loop theory. We will not go into details here.

4. 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 [5], [6], [7], [8], [10]). In a joint paper [9] 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 $n \le 63$ (cf. [2], [12]). The methods used in [2] and [12] are very detailed, and several nontrivial constructions are required to account for all the loops.

We show 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.

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 $\{(x,y) \in G\times G;\ x\cdot y \ne x*y\}$. The distance was studied extensively provided both $(G,\cdot)$, $(G,*)$ are groups, and the following results are well-known by now:

Theorem 4.1. *Let $(G,\cdot) \ne (G,*)$ be two groups of order n, and let $d = \mathrm{d}(\cdot,*)$. Then:*

(i) $d \ge 6n-24$ *when* $n \ge 51$*,*
(ii) $d \ge 6n-18$ *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 bound $d < n^2/4$ in (iv) cannot be improved. 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, $r < 7$, then there are groups $G_0 = (G,\cdot)$, G_1, …, $G_m \cong (G,*)$ such that the distance between G_i and G_{i+1} is exactly $n^2/4$ (see [1], [9]). We now reveal how the intermediate groups G_1, …, G_{m-1} are obtained. The idea works for Moufang loops, too.

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 $4m$.

Given the set $M = \{1-m,\dots,m\}$, 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

$$x * y = xyh^{\sigma(i+j)}. \tag{3}$$

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

$$x * y = xyh^{(-1)^r\sigma(i+j)}. \tag{4}$$

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 $*$.

Here are some properties of the modifications (cf. [9]).

Theorem 4.2. *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.

Using GAP [11], we have constructed all Moufang loops of order $n = 16$ and 32, and many Moufang loops of order 64 as follows: let $G_1, \ldots, G_s$ be all nonabelian groups of order n, and let $M_1, \ldots, M_s$ be the corresponding Moufang loops $M_i = M(G_i, 2)$. When $n = 16$ or $n = 32$, every nonassociative Moufang loop of order 16 is a modification of $M_1, \ldots, M_s$. The calculations for $n = 64$ are in progress. Over 3500 pairwise nonisomorphic Moufang loops of order 64 were found already.

The thesis concludes with a brief discussion of the GAP algorithms used, and of the package LOOPS [16] for GAP, currently under development by G. P. Nagy and the present author.

References

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

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

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

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

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

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

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

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

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

[10] 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.

[11] 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).

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

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

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

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

[16] 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

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

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

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

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

[21] 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.

[22] 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.

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

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

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

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

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

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

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