COMBINATORIAL ASPECTS OF CODE LOOPS

PETR VOJTĚCHOVSKÝ

Abstract. August 1, 1999. This is a very condensed form of author's talk given during LOOPS'99 conference in Prague. The construction of binary linear codes of level r (described in [5]) is introduced in a wider context of code loops, small Frattini Moufang loops, and symplectic cubic spaces. The talk was motivated by T. Hsu's paper [4].

1. Code Loops

Definition 1.1. (R. Griess, [3]) Let $F = \{0, 1\}$ be a two-element field, $C \leq F^n$ a doubly even binary linear code (i.e. $|c|$ is divisible by 4 for every codeword $c \in C$). Then $\varphi : C \times C \longrightarrow F$ is called a *factor set* if

$$\begin{aligned} \varphi(c,c) &= |c|/4, \\ \varphi(c,d) + \varphi(d,c) &= |c \cap d|/2, \\ \varphi(c,d) + \varphi(c,d+e) + \varphi(d,e) + \varphi(c+d,e) &= |c \cap d \cap e| \end{aligned}$$

for all c, d, $e \in C$. Then $(F \times C, \circ)$ is a *code loop* of C, where

$$(\alpha, c) \circ (\beta, d) = (\alpha + \beta + \varphi(c,d), c+d)$$

for every α, $\beta \in F$, c, $d \in C$.

In other words: a loop L is a code loop of C if there is a two-element central subgroup $Z \leq Z(L)$ such that L/Z is isomorphic to C as an elementary abelian 2-group.

Theorem 1.2. *(R. Griess, [3]) There is a factor set for every doubly even code C. Every two factor sets φ, ψ of C are equivalent, i.e. $(\varphi + \psi)_2$ is the zero mapping (see [5] for the definition of derived forms).*

2. How to Obtain Code Loops?

The following ideas are due to T. Hsu, [4].

Definition 2.1. *Frattini subloop* $\phi(L)$ of a loop L is the set of nongenerators of L. p-loop L is said to be *small Frattini* if $\phi(L)$ equals to 1 or p.

Lemma 2.2. *If L is a small Frattini Moufang loop then $\phi(L) \leq Z(L)$.*

Lemma 2.3. *(Chein, Goodaire [2]) For $p = 2$ the class of small Frattini Moufang loops coincides with the class of code loops.*

We will use $SFML$ instead of small Frattini Moufang loop.

3. How to Obtain SFMLs?

Again, we use results of [4].

Example 3.1. Let L be a code loop of C, $L/Z \simeq C$. Define three mappings $\sigma : C \longrightarrow Z$, $\chi : C \times C \longrightarrow Z$, $\alpha : C \times C \times C \longrightarrow Z$ by

$$\begin{aligned} \sigma(c) &= |c|/4, \\ \chi(c,d) &= |c \cap d|/2 \\ \alpha(c,d,e) &= |c \cap d \cap e|. \end{aligned}$$

Then the following identities are satisfied:

$$\begin{aligned} \sigma(nc) &= n\sigma(c), && (1) \\ \sigma(c+d) &= \begin{cases} \sigma(c)+\sigma(d)+\chi(c,d), & p=2, \\ \sigma(c)+\sigma(d), & p>2, \end{cases} && (2) \\ \chi(c,c) &= 0, && (3) \\ \chi(c,d) &= -\chi(d,c), && (4) \\ \chi(nc,d) &= n\chi(c,d), && (5) \\ \chi(c+d,e) &= \chi(c,e)+\chi(d,e)+3\alpha(c,d,e), && (6) \\ \alpha(c,d,d) &= \alpha(d,c,d) = \alpha(d,d,c) = 0, && (7) \\ \alpha(c,d,e) &= -\alpha(d,c,e) = \alpha(d,e,c), && (8) \\ \alpha(nc,d,e) &= n\alpha(c,d,e), && (9) \\ \alpha(c+d,e,f) &= \alpha(c,e,f)\alpha(d,e,f). && (10) \end{aligned}$$

In words: σ, χ, and α are power multilinear, symplectic, skew-symmetric, and related by polarization (for $p=2$). α is multilinear.

Definition 3.2. $(C, \sigma, \chi, \alpha)$ is a *symplectic cubic space* if (1)–(10) are satisfied.

Definition 3.3. *Frattini extension* of a symplectic cubic space $(C, \sigma, \chi, \alpha)$ is a loop L such that there is a central subgroup $Z \le Z(L)$ such that $L/Z \simeq C$, and

$$\begin{aligned} \sigma(c) &= \gamma^p, \\ \chi(c,d) &= [c,d], \\ \alpha(c,d,e) &= [c,d,e]. \end{aligned}$$

See [4] for details.

Theorem 3.4. *Every small Frattini Moufang loop is a Frattini extension of some symplectic cubic space, and vice versa. Moreover, given a symplectic cubic space $C = (C, \sigma, \chi, \alpha)$, there is a Frattini extension of C.*

4. How to obtain symplectic cubic spaces?

For the case $p > 2$ consult [4]. For the case $p = 2$ use the following:

Theorem 4.1. *(Chein, Goodaire [2]) Let σ_i, χ_{ij}, α_{ijk}, for $1 \le i, j, k \le m$, be arbitrary values in F. Then there is a doubly even code $C \le F^n$ with basis $\{c_1$,*

$\dots, c_m\}$ *such that*

$$\sigma(c_i) = \sigma_i,$$
$$\chi(c_i, c_j) = \chi_{ij},$$
$$\alpha(c_i, c_j, c_k) = \alpha_{ijk}.$$

5. Generalization

Let V be a vector space over F, $dim(V) < \infty$.

Definition 5.1. (M. Ashbacher [1]) Let $P : V \longrightarrow F$ be a mapping with $P(0) = 0$. Then $P_s : V^s \longrightarrow F$ defined by

$$P_s(v_1, \dots, v_s) = \sum P(v_{i_1} + \dots + v_{i_k}),$$

where the summation runs over all subsets $\{i_1, \dots, i_k\}$ of $\{1, \dots, s\}$, is called the *sth derived form* of P.

Recall the fundamental equation of derived forms:

$$\begin{aligned} P_i(u+v, v_2, \dots, v_i) &= P_i(u, v_2, \dots, v_i) + P_i(v, v_2, \dots, v_i) \\ &\quad + P_{i+1}(u, v, v_2, \dots, v_i), \end{aligned}$$

$u, v, v_2, \dots, v_i \in V$.

Since σ, χ, and α defined above are related by polarization, we have in our situation $\chi = \sigma_2$, and $\alpha = \sigma_3$. Because α is multilinear, we also have $\sigma_4 = 0$.

The problem of contructing symplectic cubic spaces described in previous section is hence equivalent to: given $P : V \longrightarrow F$ with $P(0) = 0$, $cdeg(P) = 3$, construct a doubly even binary linear code $C \simeq V$ such that

$$P(c) = |c|/4.$$

In [5], more general problem has been solved: given $P : V \longrightarrow F$ with $P(0) = 0$, $cdeg(P) = r$, construct a binary linear code $C \simeq V$ of level at least $r + 1$ (i.e. 2^{r+1} divides $|c|$ for every $c \in C$) such that

$$P(c) = |c|/2^r.$$

Here, $cdeg(P)$ denotes the combinatorial degree of P.

References

[1] M. Aschbacher, *Sporadic Groups*, Cambridge tracts in mathematics **104** (1994), Cambridge University Press

[2] O. Chein and E. Goodaire, *Moufang Loops with a Unigue Nonidentity Commutator (Associator, Square)*, J. of Algebra **130** (1990), pp. 369–384

[3] Robert L. Griess, Jr. *Code Loops*, J. of Algebra **100** (1986), pp. 224–234

[4] T. Hsu, *Moufang Loops of Class* 2 *and Cubic Forms*, Math. Proc. Camb. Phil. Soc. (to appear)

[5] Petr Vojtěchovský, *Derived Forms and Binary Linear Codes*, (to appear)

Department of Algebra, Faculty of Mathematics and Physics, Charles University, Sokolovská 83, Prague, Czech Republic

Current address: Department of Mathematics, Iowa State University, Ames, IA, U.S.A.

E-mail address: `petr@iastate.edu`