JOURNAL OF ALGEBRA **100**, 224–234 (1986)

Code Loops

ROBERT L. GRIESS, JR.

Department of Mathematics, University of Michigan,
Ann Arbor, Michigan 48109

Communicated by Walter Feit

Received June 18, 1984

Given a doubly even binary code of order 2^n, we define a code loop, a certain Moufang loop of order 2^{n+1}. It is something like "a nonassociative extraspecial 2-group." The squaring, commutation, and association relations are related to the code structure.

The first main result of this paper, Theorem 10, proves existence of the above sort of Moufang loop. The possibility of doing this was inspired by Richard Parker's recent construction of certain Moufang loops and by Conway's use of this idea in giving a new construction of the monster and its nonassociative algebra [2]. Our aim was to make a construction based on doubly even codes, which are rather familiar objects, and to thereby extend the domain of this sort of construction. Parker's approach does not involve codes. Rather, one is given a vector space V over F_2 and a subset $\mathscr{D}$ of $V-\{0\}$. Squaring, commutation, and association is based on how many vectors in certain subspaces lie in $\mathscr{D}$. A special hypothesis is that every 4-dimensional space contain evenly many elements of $\mathscr{D}$. This is satisfied by the set of dodecads in the binary Golay code; that this is so follows from Proposition 11 of this paper (we do not know of a reference for this fact in the existing literature). See Definition 13 for an exact statement. Later, we realized that Parker's construction and ours involved exactly the same objects (see Theorem 14). This coincidence was not obvious at first.

Even though we have not created any loops which did not already exist, our interpretation of these loops puts them in a natural context, hence may have some value. We know of no other published proof of the construction of this class of loops. Parker has apparently not circulated his proof. For some recent developments, see [7].

DEFINITION 1. A *loop* is a set $\mathscr{L}$ with a binary operation $\mathscr{L}\times\mathscr{L}\to\mathscr{L}$ such that $\mathscr{L}$ has an identity element and every element of $\mathscr{L}$ has a 2-sided inverse.

0021-8693/86 $3.00

Definition 2. A loop is *Moufang* if it satisfies any of these equivalent properties: (1) $xy \cdot zx = (x \cdot yz)x$; (2) $(xy \cdot z)y = x(y \cdot zy)$; (3) $x(y \cdot xz) = (xy \cdot x)z$; for all loop elements x, y, z.

We recall a basic result. See Bruck [1].

Theorem 3 (Moufang). *If a, b, c are elements of a Moufang loop and $ab \cdot c = a \cdot bc$, the subloop generated by $\{a, b, c\}$ is a group.*

Definition 4. Let V be a subspace of $P(\Omega)$, the power set of a finite set Ω regarded as a vector space over $\mathbb{F}_2$. We say that V is *doubly even* if $A \in V$ implies $|A| \equiv 0 \pmod 4$. Thus, $|A \cap B|$ is even, for $A, B \in V$.

Lemma 5. *For elements of a doubly even code,*

(i) $\frac{1}{4}|x| + \frac{1}{4}|x+y| + \frac{1}{4}|y| \equiv \frac{1}{2}|x \cap y| \pmod 2$.

(ii) $\frac{1}{4}\{|x| + |y| + |z| + |x+y| + |y+z| + |z+x| + |x+y+z|\} \equiv |x \cap y \cap z| \pmod 2$.

(iii) $\frac{1}{2}|x \cap (u+v)| + |x \cap u \cap v| = \frac{1}{2}|x \cap u| + \frac{1}{2}|x \cap v|$; $\frac{1}{2}|x \cap \sum_{i=1}^{n} u_i| + \sum_{i<j}|x \cap u_i \cap u_j| \equiv \frac{1}{2}\sum_{i=1}^{n}|x \cap u_i| \pmod 2$.

(iv) $|(x+y) \cap (u+v)| = |x \cap u| + |y \cap u| + |x \cap v| + |y \cap v| - 2(|x \cap y \cap u| + |x \cap y \cap v| + |x \cap u \cap v| + |y \cap u \cap v|) + 4|x \cap y \cap u \cap v|$.

Definition 6. Let $V \leqslant P(\Omega)$ be doubly even. A *factor set* is a function $\varphi\colon V \times V \to \mathbb{F}_2$ such that

(S) $\varphi(x, x) = \frac{1}{4}|x|$;

(C) $\varphi(x, y) + \varphi(y, x) = \frac{1}{2}|x \cap y|$;

(A) $\varphi(x, y) + \varphi(x+y, z) + \varphi(y, z) + \varphi(x, y+z) = |x \cap y \cap z|$ for all $x, y, z \in V$.

Two factor sets are *equivalent* if their difference is expressible as $\alpha(x) + \alpha(y) + \alpha(x+y)$, for some function $\alpha\colon V \to \mathbb{F}_2$ with $\alpha(0) = 0$.

Lemma 7. *For any factor set φ,*

(i) $\varphi(0, x) = \varphi(x, 0) = 0$;

(ii) $\varphi(x, y) + \varphi(x, x+y) = \frac{1}{4}|x|$;

(iii) $\varphi(b, x) + \varphi(b, x+d) + \varphi(d, x) + \varphi(d, x+b) = \frac{1}{2}|b \cap d|$, for all $x, y, b, d \in V$.

Proof. (i) In (A), set $x = 0$ to get $\varphi(0, y) + \varphi(y, z) + \varphi(y, z) + \varphi(0, y+z) = 0$, i.e., that $\varphi(0, y)$ is independent of y. Now use (A) with $x = 0$ to get $\varphi(0, y) = 0$, then (C) to get $\varphi(y, 0) = 0$.

(ii) In (A), set $y=x$ to get $\varphi(x,x)$ + $\varphi(0,z)$ + $\varphi(x,z)$ + $\varphi(x,x+z)=0$. Now use (i) and (S).

(iii) From (A), $\varphi(b,x)$ + $\varphi(b+x,d)$ + $\varphi(x,d)$ + $\varphi(b,x+d)$ = $|x\cap b\cap d|$. From (C), $\varphi(b+x,d)$ + $\varphi(d,b+x)$ = $\frac{1}{2}|d\cap(b+x)|$ = $\frac{1}{2}|d\cap b|$ + $\frac{1}{2}|d\cap b|$ + $|d\cap b\cap x|$ and $\varphi(x,d)$ + $\varphi(d,x)$ = $\frac{1}{2}|x\cap d|$.

Notation 8. (V,φ) is the set $\mathbb{F}_2\times V$ with binary compositon $(c,x)\circ(d,y)=(c+d+(x,y), x+y)$. At once, (V,φ) is a loop. We call it a *code loop.*

Proposition 9. *A code loop is a Moufang loop.*

Proof. The Moufang identity in (V,ϕ) is equivalent to

$$\varphi(x,y)+\varphi(z,x)+\varphi(x+y,z+x)=\varphi(y,z)+\varphi(x,y+z)+\varphi(x+y+z,x). \tag{1}$$

Using (A), $\varphi(x,y)$ + $\varphi(x+y,z+x)$ + $\varphi(y,z+x)$ + $\varphi(x,x+y+z)$ = $|x\cap y\cap(x+z)|$ $\equiv$ $|x\cap y\cap z|$ and so $\varphi(x,y)$ + $\varphi(x+y,z+x)$ = $\varphi(y,z+x)$ + $\varphi(x+y+z,x)$ + $|x\cap y\cap z|$ + $\frac{1}{2}|x\cap(x+y+z)|$. The last term equals $\frac{1}{2}|x\cap y|$ + $\frac{1}{2}|x\cap z|$ + $|x\cap y\cap z|$. Thus (1) is equivalent to

$$0=\varphi(z,x)+\varphi(y,z)+\varphi(x,y+z)+\varphi(y,z+x)+\tfrac{1}{2}|x\cap y|+\tfrac{1}{2}|x\cap z|. \tag{2}$$

Since $\varphi(z,x)=\varphi(x,z)+\frac{1}{2}|x\cap z|$, (2) follows from Lemma 7(iii).

Theorem 10. *Given a doubly even subspace $V\leqslant P(\Omega)$, factor sets exist. In fact, if $n=\dim V$, there are 2^{2^n-n-1} of them. Any two are equivalent.*

First Proof. Induction. Choose a chain of subspaces $V_0<V_1<\cdots<V_n=V$, with $\dim V_i=i$. Set $W_k=V_{k+1}-V_k$, for $k=0,1,\dots,n-1$. We argue by induction on k that there is φ: $V_k\times V_k\to\mathbb{F}_2$ so that (S), (C), and (A) hold.

Suppose $k=1$. Define $\varphi(x,y)=0$ if $0\in\{x,y\}$ and $\varphi(x,x)=\frac{1}{4}|x|$, for $x\in V_1-\{0\}$.

We now suppose that $n-1\geqslant k\geqslant 0$ and that φ has been defined on $V_k\times V_k$ and satisfies (S), (C), and (A). We choose $x\in W_k$. Consider the axioms

(Q) $\varphi(x,y)+\varphi(x,x+y)=\frac{1}{4}|x|$;

(R) $\varphi(b,x)+\varphi(b,x+d)+\varphi(d,x)+\varphi(d,x+b)=\frac{1}{2}|b\cap d|$.

These are taken from Lemma 7, and we use them to define φ on $V_{k+1}\times V_{k+1}$. The definition proceeds in steps.

(D1) Define φ arbitrarily on $\{x\} \times V_k$, but make $\varphi(x, 0) = 0$; deduce the values of φ on $V_k \times \{x\}$ using (C).

(D2) Deduce φ on $\{x\} \times W_k$ by imposing (Q) and deduce φ on $W_k \times \{x\}$ from (C).

(D3) Deduce φ on $W_k \times W_k$ by using (R) with $b \in V_k$, $d \in W_k$.

(D4) Deduce φ on $W_k \times V_k$ by using (Q) with x representing an arbitrary element of W_k and $y \in V_k$; deduce φ on $V_k \times W_k$ using (C).

We must now check that (S), (C), and (A) hold for this φ defined on $V_{k+1} \times V_{k+1}$.

(S): From (D2), $\varphi(x, 0) + \varphi(x, x) = \frac{1}{4}|x|$ and $\varphi(x, 0) = 0$ from (D1). Now take $d = x + b \in W_k$, $b \in V_k$. From (D3), $\varphi(d, d) = \varphi(b, x) + \varphi(b, b) + \varphi(b + x, x) + \frac{1}{2}|b \cap (b + x)|$. From (D1) and (D2), $\varphi(b, x) + \varphi(b + x, x) = \varphi(x, b) + \varphi(x, x + b) = \frac{1}{4}|x|$. So, $\varphi(d, d) = \frac{1}{4}|d|$ because $\varphi(b, b) = \frac{1}{4}|b|$, by induction, and $\frac{1}{2}|b \cap (b + x)| = \frac{1}{2}|b \cap x|$ and by Lemma 5(i).

(C): $\varphi(a, b) + \varphi(b, a) = \frac{1}{2}|a \cap b|$ holds by induction or by definition, unless $a, b \in W_k$. Assume, then, that $a, b \in W_k$. By (D3), $\varphi(a, b)$ and $\varphi(b, a)$ were defined by

$$\varphi(b + x, x) + \varphi(b + x, x + a) + \varphi(a, x) + \varphi(a, b) = \tfrac{1}{2}|(b + x) \cap a|, \tag{1}$$

$$\varphi(a + x, x) + \varphi(a + x, x + b) + \varphi(b, x) + \varphi(b, a) = \tfrac{1}{2}|(a + x) \cap b|, \tag{2}$$

respectively. Let $R_1, ..., R_8$ denote the eight summands on the left side. From (D1), $R_1 + R_7 = \frac{1}{4}|x|$ and $R_3 + R_5 = \frac{1}{4}|x|$. By induction, $R_2 + R_6 = \frac{1}{2}|(a + x) \cap (b + x)|$, which by Lemma 5(iv) equals $\frac{1}{2}|x \cap b| + \frac{1}{2}|a \cap x| + \frac{1}{2}|a \cap b|$. Summing (1) and (2) and simplifying their right sides, we get $\varphi(a, b) + \varphi(b, a) = \frac{1}{2}|a \cap b|$, as required.

(A): This is the hardest axiom to check. Define $A(a, b, c) = \varphi(a, b) + \varphi(a + b, c) + \varphi(b, c) + \varphi(a, b + c)$. By induction $A(a, b, c) = |a \cap b \cap c|$ for a, b, $c \in V_k$. For a, b, $c \in V_{k+1}$, $A(a, b, c) + A(b, c, a) + A(c, a, b) = \varphi(a + b, c) + \varphi(b + c, a) + \varphi(c + a, b) + \varphi(a, b + c) + \varphi(b, c + a) + \varphi(c, a + b)$. Since (C) holds, this simplifies to

$$A(a, b, c) + A(b, c, a) + A(c, a, b) = |a \cap b \cap c|, \tag{3}$$

using Lemma 5(iii). We shall prove (A) by studying cases, and (3) will cut down the work.

Case 1. a, b, $c \in W_k$. By definition of $\varphi(a, b)$ and $\varphi(b, c)$, from (D3),

$$\varphi(b + x, x) + \varphi(b + x, x + a) + \varphi(a, x) + \varphi(a, b) = \tfrac{1}{2}|(b + x) \cap a| \tag{4}$$

$$\varphi(c + x, x) + \varphi(c + x, x + b) + \varphi(b, x) = \tfrac{1}{2}|(c + x) \cap b|. \tag{5}$$

From (D4), $\varphi(a+b, c) = \frac{1}{2}|(a+b)\cap c| + \varphi(c, a+b) = \frac{1}{2}|(a+b)\cap c| + \varphi(c, a+b+c) + \frac{1}{4}|c|$ and $\varphi(a, b+c) = \varphi(a, a+b+c) + \frac{1}{4}|a|$. From (D3),

$$\varphi(a+b+c+x, x) + \varphi(a+b+c+x, x+a) + \varphi(a, x) + \varphi(a, a+b+c) = \tfrac{1}{2}|a\cap(b+c+x)| \tag{6}$$

$$\varphi(a+b+c+x, x) + \varphi(a+b+c+x, x+c) + \varphi(c, x) + \varphi(c, a+b+c) = \tfrac{1}{2}|c\cap(a+b+x)|. \tag{7}$$

Define $T = \varphi(b+x, x+a) + \varphi(c+x, x+b) + \varphi(a+b+c+x, x+a) + \varphi(a+b+c+x, x+c)$ and $U = \frac{1}{2}|(b+x)\cap a| + \frac{1}{2}|(c+x)\cap b| + \frac{1}{2}|a\cap(b+c+x)| + \frac{1}{2}|c\cap(a+b+x)| + \frac{1}{2}|(a+b)\cap c| + \frac{1}{4}|c| + \frac{1}{4}|a|$, which, by Lemma 5(iii), equals $\frac{1}{4}|c| + \frac{1}{4}|a| + \frac{1}{2}|x\cap b| + \frac{1}{2}|x\cap c| + |b\cap x\cap a| + |c\cap x\cap b| + |a\cap b\cap c| + |a\cap b\cap x| + |a\cap c\cap x| + |c\cap a\cap b| + |c\cap a\cap x| + |c\cap b\cap x| + \frac{1}{2}|(a+b)\cap c| = \frac{1}{4}|c| + \frac{1}{4}|a| + \frac{1}{2}|x\cap b| + \frac{1}{2}|x\cap c| + \frac{1}{2}|a\cap c| + \frac{1}{2}|b\cap c| + |a\cap b\cap c|$. Then, using $\varphi(b+x, x) + \varphi(b, x) = \frac{1}{4}|x| = \varphi(c+x, x) + \varphi(c, x)$, we get $A(a, b, c) = T + U$.

Since $r = x+a$, $s = x+b$, and $t = x+c$ are in V_k, we may evaluate T by induction. We have $T = \varphi(s, r) + \varphi(t, s) + \varphi(r+s+t, r) + \varphi(r+s+t, t)$. By induction, $\varphi(r+s+t, r) = \varphi(r, r+s+t) + \frac{1}{2}|r\cap(s+t)| = \varphi(r, s+t) + \frac{1}{4}|r| + \frac{1}{2}|r\cap(s+t)| = \varphi(s+t, r) + \frac{1}{4}|r|$ and $\varphi(r+s+t, t) = \varphi(r+s, t) + \frac{1}{4}|t| = \varphi(t, r+s) + \frac{1}{2}|(r+s)\cap t| + \frac{1}{4}|t|$. Therefore, $T = A(t, s, r) + \frac{1}{4}|t| + \frac{1}{4}|r| + \frac{1}{2}|t\cap(r+s)| = |t\cap s\cap r| + \frac{1}{4}|t| + \frac{1}{4}|r| + \frac{1}{2}|t\cap(r+s)| = \frac{1}{4}|t| + \frac{1}{4}|r| + \frac{1}{2}|t\cap r| + \frac{1}{2}|t\cap s| = \frac{1}{4}|x+c| + \frac{1}{4}|x+a| + \frac{1}{2}|(x+c)\cap(x+a)| + \frac{1}{2}|(x+c)\cap(x+b)| = \frac{1}{4}|c| + \frac{1}{4}|a| + \frac{1}{2}|x\cap c| + \frac{1}{2}|x\cap a| + \frac{1}{2}|x\cap a| + \frac{1}{2}|x\cap c| + \frac{1}{2}|a\cap c| + \frac{1}{2}|x\cap b| + \frac{1}{2}|x\cap c| + \frac{1}{2}|b\cap c| = \frac{1}{4}|c| + \frac{1}{4}|a| + \frac{1}{2}|a\cap c| + \frac{1}{2}|x\cap b| + \frac{1}{2}|x\cap c| + \frac{1}{2}|b\cap c|$. We conclude that $A(a, b, c) = T + U = |a\cap b\cap c|$, as required.

Case 2. a, $c \in V_k$, $b \in W_k$. Set $x = a+b+c$, $y = a+b$, $z = b$. Case 1 for x, y, z gives $|a\cap b\cap c| = A(a+b+c, a+b, b)$. Using (D4), we get

$$\begin{aligned}\varphi(a, b+c) &= \varphi(a, a+b+c) + \tfrac{1}{4}|a| \\ &= \varphi(a+b+c, a) + \tfrac{1}{4}|a| + \tfrac{1}{2}|a\cap(b+c)|\end{aligned} \tag{8}$$

$$\begin{aligned}\varphi(a+b, c) &= \varphi(a+b, a+b+c) + \tfrac{1}{4}|a+b| \\ &= \varphi(a+b+c, a+b) + \tfrac{1}{4}|a+b| + \tfrac{1}{2}|(a+b)\cap c|\end{aligned} \tag{9}$$

$$\begin{aligned}\varphi(a, b) &= \varphi(b, a) + \tfrac{1}{2}|a\cap b| \\ &= \varphi(b, a+b) + \tfrac{1}{4}|b| + \tfrac{1}{2}|a\cap b| = \varphi(a+b, b) + \tfrac{1}{4}|b|.\end{aligned} \tag{10}$$

Therefore, $A(a, b, c) = A(a+b+c, a+b, b) + \frac{1}{4}|b| + \frac{1}{4}|a| + \frac{1}{4}|a+b| + \frac{1}{2}|a\cap(b+c)| + \frac{1}{2}|(a+b)\cap c| + \frac{1}{2}|b\cap c|$ (the last summand is the price for changing $\varphi(c, b)$ to $\varphi(b, c)$), and $A(a, b, c) = |a\cap b\cap c|$.

Case 3. $a \in W_k$, b, $c \in V_k$. From (D4),

$$\varphi(a, b) + \varphi(a, a+b) = \tfrac{1}{4}|a| \tag{11}$$

$$\varphi(a, b+c) + \varphi(a, a+b+c) = \tfrac{1}{4}|a| \tag{12}$$

$$\varphi(a+b, c) + \varphi(a+b, a+b+c) = \tfrac{1}{4}|a+b|. \tag{13}$$

Thus, $A(a, b, c) = \varphi(a, a+b) + \varphi(a+b, a+b+c) + \varphi(b, c) + \varphi(a, a+b+c) + \frac{1}{4}|a+b|$. We now refer to (D3) to get

$$\begin{aligned}&\varphi(a+b+x, x) + \varphi(a+b+x, x+a) + \varphi(a, x) + \varphi(a, a+b)\\ &\quad = \tfrac{1}{2}|(b+x) \cap a| \qquad (14)\\ &\varphi(a+b+c+x, x) + \varphi(a+b+c+x, a+b+x)\\ &\qquad + \varphi(a+b, x) + \varphi(a+b, a+b+c)\\ &\quad = \tfrac{1}{2}|(c+x) \cap (a+b)| \qquad (15)\\ &\varphi(a+b+c+x, x) + \varphi(a+b+c+x, x+a) + \varphi(a, x) + \varphi(a, a+b+c)\\ &\quad = \tfrac{1}{2}|(b+c+x) \cap a|. \qquad (16)\end{aligned}$$

Let R_{ij} be the (i, j) term on the left sides of these equations, $i = 1, 2, 3$, $j = 1, 2, 3, 4$. From (C) and (D4), $R_{11} + R_{23} = \frac{1}{4}|x|$. Also, $R_{13} = R_{33}$ and $R_{21} = R_{31}$. Now set $u = a+b+x$, $v = a+x$. Since u, v, $c \in V_k$, we have by induction that $\varphi(v, u) + \varphi(v, u+c) + \varphi(c, u) + \varphi(c, u+v) = \frac{1}{2}|v \cap c|$. Note that $R_{12} = \varphi(v, u) + \frac{1}{2}|u \cap v|$, $R_{32} = \varphi(v, u+c) + \frac{1}{2}|(u+c) \cap v|$, $R_{22} = \varphi(c, u) + \frac{1}{4}|u|$, $\varphi(c, u+v) = \varphi(c, b) = \varphi(b, c) + \frac{1}{2}|b \cap c|$. Therefore, $R_{14} + R_{24} + R_{34} = \frac{1}{4}|x| + \frac{1}{2}|v \cap c| + \frac{1}{2}|u \cap v| + \frac{1}{2}|(u+c) \cap v| + \frac{1}{4}|u| + \frac{1}{2}|(b \cap c)| + \varphi(b, c) + \frac{1}{2}|(b+x) \cap a| + \frac{1}{2}|(c+x) \cap (a+b)| + \frac{1}{2}|(b+c+x) \cap a| = \frac{1}{4}|x| + |u \cap v \cap c| + \frac{1}{4}|u| + \frac{1}{2}|b \cap c| + \varphi(b, c) + \frac{1}{2}|b \cap a| + \frac{1}{2}|x \cap a| + |b \cap x \cap a| + \frac{1}{2}|(c+x) \cap a| + \frac{1}{2}|(c+x) \cap b| + |(c+x) \cap a \cap b| + \frac{1}{2}|b \cap a| + \frac{1}{2}|(c+x) \cap a| + \frac{1}{2}|b \cap a| + |(c+x) \cap a \cap b| = \frac{1}{4}|x| + |b \cap a \cap c| + |b \cap x \cap c| + \frac{1}{4}|a+b+x| + \frac{1}{2}|b \cap c| + \varphi(b, c) + \frac{1}{2}|x \cap a| + |b \cap x \cap a| + \frac{1}{2}|(c+x) \cap b| = \frac{1}{4}|a+b| + \frac{1}{2}|a \cap x| + \frac{1}{2}|b \cap x| + |a \cap b \cap x| + |b \cap a \cap c| + |b \cap x \cap c| + \frac{1}{2}|b \cap c| + \varphi(b, c) + \frac{1}{2}|x \cap a| + |b \cap x \cap a| + \frac{1}{2}|c \cap b| + \frac{1}{2}|x \cap b| + |c \cap x \cap b| = \frac{1}{4}|a+b| + |a \cap b \cap c| + \varphi(b, c)$. It follows that $A(a, b, c) = |a \cap b \cap c|$, as required.

Case 4. $c \in W_k$, a, $b \in V_k$. $A(a, b, c) = |a \cap b \cap c|$ follows from (3) and Cases 2 and 3.

Case 5. a, $b \in W_k$, $c \in V_k$. Case 3 applied to $x = a$, $y = a+b+c$, $z = c$ gives $|a \cap b \cap c| = A(a, a+b+c, c)$. By (D4), $\varphi(a, a+b+c) = \varphi(a, b+c) + \frac{1}{4}|a|$ and $\varphi(b+c, c) = \varphi(b+c, b) + \frac{1}{4}|b+c| = \varphi(b, b+c) + \frac{1}{2}|b \cap c| + \frac{1}{4}|b+c| = \varphi(b, c) + \frac{1}{4}|c|$. By induction, $\varphi(a+b+c, c) =$

$\varphi(c, a+b+c) + \frac{1}{2}|(a+b)\cap c| = \varphi(c, a+b) + \frac{1}{4}|c| + \frac{1}{2}|(a+b)\cap c| = \varphi(a+b, c) + \frac{1}{4}|c|$. Again, by (D4), $\varphi(a, a+b) = \varphi(a, b) + \frac{1}{4}|a|$. Thus, $A(a, a+b+c, c) = A(a, b, c)$.

Case 6. $a \in V_k$, $b, c \in W_k$. The same argument as Case 5, except that we employ (C) in slightly different ways to use (D4).

Case 7. $a, c \in W_k$, $b \in V_k$. Use Cases 5 and 6 and (3).

This completes the induction step.

We now prove that two factor sets are equivalent. If $\zeta(x, y)$ denotes the difference of two factor sets, $\zeta\colon V \times V \to \mathbb{F}_2$ satisfies $\zeta(x, x) = 0$, $\zeta(x, y) + \zeta(y, x) = 0$, and $\zeta(x, y) + \zeta(x+y, z) + \zeta(y, z) + \zeta(x, y+z) = 0$ for all $x, y, z \in V$. Thus, ζ is a 2-cocycle which gives an elementary abelian group as an extension of V by $\mathbb{F}_2$, hence ζ is cohomologous to 0, i.e., there is $\alpha\colon V \to \mathbb{F}_2$ with $\zeta(x, y) = \alpha(x) + \alpha(y) + \alpha(x+y)$. Thus, our two factor sets are equivalent.

The number of factor sets is, from n applications of (D1), $2^{A(n)}$, where $A(n) = \sum_{i=1}^{n} (2^{i-1} - 1) = 2^n - 1 - n$. The previous paragraph suggests that $A(n)$ might be $2^n - 1$. The difference of n is explained by the fact that replacement of a factor set $\varphi(x, y)$ by $\varphi(x, y) + \alpha(x) + \alpha(y) + \alpha(x+y)$ results in no change precisely when $\alpha\colon V \to \mathbb{F}_2$ is a homomorphism.

Second Proof. H. N. Ward was so kind as to supply an existence proof for factor sets by using a calculus described in his paper [6]. In the notation of [6], we are looking for a function ϕ such that

$$\begin{aligned} \varphi(x, x) &= q(x) \\ \varphi(x, y) + \varphi(y, x) &= dq(x, y) \qquad (*) \\ \varphi(x, y) + \varphi(x+y, z) + \varphi(y, z) + \varphi(x, y+z) &= dq(x, y, z), \end{aligned}$$

where $q(x) = \frac{1}{4}|x|$, for $x \in V$ (see Lemma 5). Notice that $dq(w, x, y, z) = 0$ (see Proposition 11). Thus, the combinatorial degree of q and the polynomial degree of q are at most 3. Since $q(0) = 0$, q is a linear combination of λ_1, $\lambda_1\lambda_2$, and $\lambda_1\lambda_2\lambda_3$, where $\lambda_i \in V^*$. Define $x_i = \lambda_i(x)$ for $x \in V$. Then, using 2.5 of [6],

$$\begin{aligned} &dp(x, y) = 0 \qquad \text{if} \quad p = \lambda_1; \\ &dp(x, y) = x_1 y_2 + x_2 y_1 \end{aligned}$$

and

$$\begin{aligned} dp(x, y, z) &= 0 \qquad \text{if} \quad p = \lambda_1\lambda_2; \\ dp(x, y) &= x_1 x_2 y_3 + x_1 y_2 x_3 + y_1 x_2 x_3 \\ &\quad + x_1 y_2 y_3 + y_1 x_2 y_3 + y_1 y_2 x_3 \end{aligned}$$

and

$$dp(x, y, z) = \sum_{\{i,j,k\} = \{1,2,3\}} x_i y_j z_k \qquad \text{if} \quad p = \lambda_1 \lambda_2 \lambda_3.$$

If $p = \lambda_1$, $\lambda_1 \lambda_2$, or $\lambda_1 \lambda_2 \lambda_3$ replaces q on the right side of $(*)$, then $\phi(x, y) = x_1$, $x_1 y_2$, or $x_1 y_2 y_3 + y_1 x_2 y + y_1 y_2 x_3$, respectively, is a solution. Since q is a linear combination of such p, the correponding linear combination of the respective φ solves $(*)$.

We finish as in the First Proof.

We now record an elementary property of doubly even codes.

PROPOSITION 11. *If* $\dim V \geqslant 4$, $\sum_{v \in V} \varphi(v, v) = 0$.

Proof. Write $V = U \bigoplus W$, where $\dim U = 2$. For $w \in W$, $w \neq 0$, let $S(w)$ be the 3-space $\operatorname{span}\{U, w\}$. If $v \in V$, $|\{w \in W - \{0\} \mid v \in S(w)\}|$ is 1 or $|W| - 1$; both numbers are odd. For $S \subseteq V$, let $a(S) = \sum_{v \in S} \varphi(v, v)$. Then $a(V) = \sum_{w \in W - \{0\}} a(S(w))$. Let $\{u_1, u_2\}$ be a basis of U. By Lemma 5(ii), $a(S(w)) = |w \cap u_1 \cap u_2|$. Therefore, since $\dim W \geqslant 2$, $a(V) = |(\sum_{w \in W - \{0\}} w) \cap u_1 \cap u_2| = |0 \cap u_1 \cap u_2| = 0$.

DEFINITION 12. Let $\mathscr{L}$ be a loop. We say that $\mathscr{L}$ is *afforded by the code* V if V is a binary, doubly even code and there is a factor set φ such that $\mathscr{L} \cong (V, \varphi)$. We also say that V *affords* $\mathscr{L}$.

We now proceed to the setup considered by Parker. The model for this definition is the case where V is the binary Golay code and $\mathscr{D}$ is the family of 2576 dodecads in V.

DEFINITION 13. Let V be any finite-dimensional vector space over F_2. Let $\mathscr{D}$ be any subset of $V - \{0\}$. A *Parker function* is a function p: $V \times V \to F_2$ such that

(S) $p(x, x) = |x \cap \mathscr{D}|$;

(C) $p(x, y) + p(y, x) = \sum_{i,j \in F_2} |(ix + jy) \cap \mathscr{D}|$;

(A) $p(x, y) + p(x + y, z) + p(y, z) + p(x, y + z) = \sum_{i,j,k \in F_2} |(ix + jy + kz) \cap \mathscr{D}|$.

The associated *Parker loop* is (V, p), the set $F_2 \times V$ with binary composition $(c, x) \circ (d, y) = (c + d + p(x, y), x + y)$.

We write $p(x)$ or $q(x)$ for $p(x, x)$. Notice that the right sides of (C), (A) are 0 if $\{x, y\}$, $\{x, y, z\}$, respectively, are linearly dependent. Also, write $q(x, y)$ for $\sum_{i,j \in F_2} p(ix + jy)$ and $q(x, y, z)$ for $\sum_{i,j,k \in F_2} p(ix + jy + kz)$.

The *Parker condition* is the requirement that, for any 4-dimensional subspace $U \leqslant V$, $\sum_{x \in U} p(x) = 0$.

THEOREM 14. *If V satisfies the Parker condition, the Parker loop (V, p) is a code loop. More precisely, there is a doubly even code W, a linear isomorphism $\alpha\colon V \to W$, and a factor set φ on W such that $(c, v) \leftrightarrow (c, \alpha(v))$ gives an isomorphism of loops $(V, p) \cong (W, \varphi)$. In particular, (V, p) is a Moufang loop. Conversely, a code loop is a Parker loop satisfying the Parker condition.*

This theorem shows that the loops obtained by the apparently special conditions of Parker's construction are identical to those coming from the rather natural-looking doubly even code construction of Proposition 9. The converse is trivial to prove, since we take $\mathscr{D}$ to be the family of sets in the code with cardinality 4 (mod 8), then quote Proposition 11.

The code affording (V, p) is certainly not unique. Let $C \leqslant P(\Omega)$ be such a code and let Γ be a set, $|\Gamma| \equiv 0 \pmod 8$, $\Omega \cap \Gamma = \varnothing$. Take any nonzero linear map $f\colon C \to F_2$ and define $C' \leqslant P(\Omega \cup \Gamma)$ as the set of all $x + f(x)\,\Gamma$, for $x \in C$. Then C' affords (V, p) and $C' \ncong C$.

Before proving the Theorem, we need a lemma.

LEMMA 15. *If the Parker condition holds, $q(x, y, z)$ is trilinear.*

Proof. Suppose that $z = z_1 + z_2$. Without loss, $\{x, y\}$ is independent.

Suppose that all of $\{x, y, z\}$, $\{x, y, z_1\}$, and $\{x, y, z_2\}$ are independent. Then $\{x, y, z_1, z_2\}$ spans a 4-space, U. We have $q(x, y, z) + q(x, y, z_1) + q(x, y, z_2) = \sum_{t \in U} p(t) = 0$, whence linearity in this case.

If not all three sets are independent, then oddly many are dependent and q vanishes on these, whence dependence since the remaining sets span the same 3-space.

We are done by symmetry.

Proof of Theorem 14. We induct on dim V. If dim $V = 0$, the argument is trivial and if dim $V = 1$, say, $V = \{0, x\}$, just take an 8-set or a 4-set, A, as $p(x) = 0$ or 1 and let $W = \{0, A\} \leqslant P(A)$.

Now let $k \geqslant 1$ and take a basis $x_1, \dots, x_{k+1}$ for V. Set $U = \operatorname{span}\{x_1, \dots, x_k\}$. By induction, there are a finite set Ω, a doubly even subspace $W \leqslant P(\Omega)$, a factor set φ on W, and a linear isomorphism $\alpha\colon U \to W$ such that $p(u_1, u_2) = \varphi(\alpha(u_1), \alpha(u_2))$, for $u_1, u_2 \in U$.

For $i, j = 1, \dots, k$, $i \neq j$, let Ω_i be an 8-set and Ω_{ij} an 8-set and Ω_{k+1} an 8-set, with all of Ω_i, Ω_{ij} mutually disjoint and disjoint from Ω. Define

$$B_i = \alpha(x_i) \cup \Omega_i \cup \bigcup_{\substack{j=1 \\ j \neq i}}^{k} \Omega_{ij}$$

and $c_i = p(x_i, x_{k+1}) + p(x_{k+1}, x_i)$, for $i = 1, \dots, k$. Define $d_{ij} = q(x_i, x_j, x_{k+1})$, $i \neq j$, $1 \leqslant i, j \leqslant k$. For $i \neq j$ in $\{1, \dots, k\}$ take $A_{ij} \subseteq \Omega_{ij}$ to be a set of cardinality d_{ij} (mod 2). Then take $A_i \subseteq \Omega_i$, $i=1,..., k$, so that $\frac{1}{2}|A_i \cup \bigcup_{j\neq i} A_{ij}| = c_i$ (mod 2). Finally, take $A_{k+1} \subseteq \Omega_{k+1}$ so that

$$A = \bigcup_{i=1}^{k+1} A_i \cup \bigcup_{\substack{i\neq j \\ i,j=1,...,k}} A_{ij}$$

satisfies $\frac{1}{4}|A| = p(x_{k+1})$ (mod 2).

Let Ω' be the union of Ω and all the Ω_i and Ω_{ij}. Set $W' = \operatorname{span}\{B_1,..., B_k, A\} \leqslant P(\Omega')$. The space W' is doubly even since the basis elements have cardinality 0 (mod 4) and the intersection of any two is an even set. We define a linear isomorphism α': $V \to W'$ by $\alpha'(x_i) = B_i$, $i = 1,..., k$, and $\alpha'(x_{k+1}) = A$.

We now prove that

$$\tfrac{1}{4}|\alpha(v)| = p(v) \qquad \text{for} \quad v \in V; \tag{1}$$

and

$$p(u, x_{k+1}) + p(x_{k+1}, u) = \tfrac{1}{2}|\alpha'(u) \cap A| \qquad \text{for} \quad x \in V - U,\ u \in U. \tag{2}$$

By induction on k, it suffices to check (1) for v of the form $u + x_{k+1}$, $u \in U$. We prove (1) and (2) by induction on the cardinality of $\operatorname{supp}(u) =$ the set of i appearing in an expression of u as a linear combination of $x_1,..., x_k$.

If $|\operatorname{supp}(u)| \leqslant 1$, (1) and (2) follow by the definitions. Now suppose $|\operatorname{supp}(u)| \geqslant 2$. Write $u = u_1 + u_2$ where $|\operatorname{supp}(u_i)| < |\operatorname{supp}(u)|$, $i = 1, 2$.

The functions $q(x, y, z)$ and $q'(x, y, z) = |\alpha'(x) \cap \alpha'(y) \cap \alpha'(z)|$ are both trilinear (Lemmas 5 and 15), and both alternating. We agrue that they are equal, and it suffices to check them on triples (x_i, x_j, x_l), $i < j < l$. By induction, we may even assume that $l = k+1$. On such triples, we have equality since A was arranged to satisfy $|A \cap B_i \cap B_j| = d_{ij}$ (mod 2).

We have $q(u_1, u_2, x) = \sum_{i,j,l \in F_2} p(iu_1 + ju_2 + lx_{k+1})$. If $(i, j, l) \neq (1, 1, 1)$, we have $p(iu_1 + ju_2 + lx_{k+1}) = \frac{1}{4}|\alpha'(iu_1 + ju_2 + lx_{k+1})|$, by induction on k or on the cardinality of support. The previous paragraph now gives equality at (1, 1, 1). So, (1) holds.

To get (2), we argue as follows. From (C), $p(u, x_{k+1}) + p(x_{k+1}, u) = \sum_{i,j \in F_2} p(ix_{k+1} + ju) = q(u_1, u_2, x_{k+1}) + q(u_1, x_{k+1}) + q(u_2, x_{k+1}) = |\alpha'(u_1) \cap \alpha'(u_2) \cap A| + \frac{1}{2}|\alpha'(u_1) \cap A| + \frac{1}{2}|\alpha'(u_2) \cap A|$, by induction. By Lemma 5(iii), the right side equals $\frac{1}{2}|\alpha'(u) \cap A|$, proving (2).

It follows from (1) that $\varphi'(x, y) = p(\alpha'^{-1}(x), \alpha'^{-1}(y))$ is a factor set on W'. At once, $(V, p) \cong (W', \varphi')$ via $(c, v) \leftrightarrow (c, \alpha'(v))$. Since (W', φ') is a Moufang loop, all parts of Theorem 14 are proven.

EXAMPLE 16. Let $\dim V = 3$ and $D = V - \{0\}$. The loop $\mathscr{L}$ afforded by

V has order 2^4. The eight pairs $\{\pm x\}$, $x \in \mathscr{L}$, form a double basis for the Cayley number, $\mathscr{C}$. $\mathrm{Aut}(\mathscr{L})$ is a nonsplit extension $2^3 \cdot L_3(2)$, and it is well known that $\mathrm{Aut}(\mathscr{L}) \leqslant \mathrm{Aut}(\mathscr{C})$, whose complexified form is $G_2(\mathbb{C})$. See [7] for full details on this.

We show that $\mathscr{L}$ is afforded by a code. Take $\Omega = \{1, 2, ..., 7\}$, and let $V \leqslant P(\Omega)$ be the span of $\{1, 2, 3, 4\}$, $\{3, 4, 5, 6\}$, $\{1, 3, 5, 7\}$. Every nonzero set in V has cardinality 4.

The procedure of Theorem 14 for finding a suitable Ω constructs one of cardinality 38. Evidently, that procedure is not best-possible.

References

1. R. H. Bruck, "A Survey of Binary Systems," Springer–Verlag, Berlin, 1968.
2. J. Conway, privately circulated notes, 1984.
3. R. L. Griess, Jr., A construction of F as automorphisms of a 196883 dimensional algebra, *Proc. Nat. Acad. Sci. U.S.A* **78** (1981), 689–691.
4. R. L. Griess, Jr., The friendly giant, *Invent. Math.* **69** (1982), 1–102.
5. R. L. Griess, Jr., The monster and its nonassociative algebra, *in* "Proceedings, Montreal 1982 Finite Group Theory Conference" (John McKay, Ed.), in press.
6. N. Ward, Combinatorial polarizaton, *Discrete Math.* **26** (1979), 185–197.
7. R. L. Griess, Jr., Sporadic groups, code loops and nonvanishing cohomology, to appear in *J. Pure Appl. Algebra.*