257
169
16
LA-3996

595
MASTER

LOS ALAMOS SCIENTIFIC LABORATORY
of the
University of California
LOS ALAMOS • NEW MEXICO

Veblen-Wedderburn Systems

UNITED STATES
ATOMIC ENERGY COMMISSION
CONTRACT W-7405-ENG. 36

DISTRIBUTION OF THIS DOCUMENT IS UNLIMITED

DISCLAIMER

This report was prepared as an account of work sponsored by an agency of the United States Government. Neither the United States Government nor any agency Thereof, nor any of their employees, makes any warranty, express or implied, or assumes any legal liability or responsibility for the accuracy, completeness, or usefulness of any information, apparatus, product, or process disclosed, or represents that its use would not infringe privately owned rights. Reference herein to any specific commercial product, process, or service by trade name, trademark, manufacturer, or otherwise does not necessarily constitute or imply its endorsement, recommendation, or favoring by the United States Government or any agency thereof. The views and opinions of authors expressed herein do not necessarily state or reflect those of the United States Government or any agency thereof.

DISCLAIMER

Portions of this document may be illegible in electronic image products. Images are produced from the best available original document.

LEGAL NOTICE

This report was prepared as an account of Government sponsored work. Neither the United States, nor the Commission, nor any person acting on behalf of the Commission:

A. Makes any warranty or representation, expressed or implied, with respect to the accuracy, completeness, or usefulness of the information contained in this report, or that the use of any information, apparatus, method, or process disclosed in this report may not infringe privately owned rights; or

B. Assumes any liabilities with respect to the use of, or for damages resulting from the use of any information, apparatus, method, or process disclosed in this report.

As used in the above, "person acting on behalf of the Commission" includes any employee or contractor of the Commission, or employee of such contractor, to the extent that such employee or contractor of the Commission, or employee of such contractor prepares, disseminates, or provides access to, any information pursuant to his employment or contract with the Commission, or his employment with such contractor.

This report expresses the opinions of the author or authors and does not necessarily reflect the opinions or views of the Los Alamos Scientific Laboratory.

Printed in the United States of America. Available from
Clearinghouse for Federal Scientific and Technical Information
National Bureau of Standards, U. S. Department of Commerce
Springfield, Virginia 22151

Price: Printed Copy \$3.00; Microfiche \$0.65

LA-3996

UC-32, MATHEMATICS
AND COMPUTERS
TID-4500

LOS ALAMOS SCIENTIFIC LABORATORY
of the
University of California
LOS ALAMOS • NEW MEXICO

Report written: August 1968

Report distributed: December 20, 1968

Veblen-Wedderburn Systems

by

C. J. Everett

LEGAL NOTICE

This report was prepared as an account of Government sponsored work. Neither the United States, nor the Commission, nor any person acting on behalf of the Commission:

A. Makes any warranty or representation, expressed or implied, with respect to the accuracy, completeness, or usefulness of the information contained in this report, or that the use of any information, apparatus, method, or process disclosed in this report may not infringe privately owned rights; or

B. Assumes any liabilities with respect to the use of, or for damages resulting from the use of any information, apparatus, method, or process disclosed in this report.

As used in the above, "person acting on behalf of the Commission" includes any employee or contractor of the Commission, or employee of such contractor, to the extent that such employee or contractor of the Commission, or employee of such contractor prepares, disseminates, or provides access to, any information pursuant to his employment or contract with the Commission, or his employment with such contractor.

**THIS PAGE
WAS INTENTIONALLY
LEFT BLANK**

VEBLEN-WEDDERBURN SYSTEMS

by

C. J. Everett

ABSTRACT

It is shown that Veblen-Wedderburn systems of order $N = p^n$, not division rings, exist for every $p \geq 2$, $n \geq 2$, for p an odd prime, and for $p = 2$, n composite. The proof suggests a matrix algorithm for constructing all V-W systems. The method is carried through for $p = 3$, $n = 2$ and reveals 5 such nonisomorphic systems. Some orienting remarks of an expository nature are included as an introduction to these structures and to their relation to the combinatorial configurations known as finite planes.

1. Veblen-Wedderburn Systems. Let $R, +$ be a finite additive group of order $N \geq 2$, closed under an operation xy such that

$$R1. \quad x(y+z) \equiv xy + xz$$

$$R2. \quad \text{for } z \neq 0, \text{ the map } x \rightarrow xz \text{ is one-one.}$$

Consideration of the products $x(y+0)$ and $x(-y)$ under R1 shows that

$$C1. \quad x \cdot 0 \equiv 0 \qquad C2. \quad x(-y) \equiv -(xy).$$

Hence also

$$C3. \quad \text{if } m \neq m', \text{ the map } x \rightarrow -m'x + mx \text{ is one-one.}$$

For, $-m'x_1 + mx_1 = -m'x_2 + mx_2$ implies $m'(x_2 - x_1) = m(x_2 - x_1)$, and $x_2 - x_1 = 0$ follows from R2.

Taking the pairs (x, y) as points of a plane $\pi(R)$, and all the sets $\ell[a] = \{(a, y); y \in R\}$, $\ell[m, k] = \{(x, mx+k); x \in R\}$ as lines, it is easy to verify the axioms for a finite affine plane π :

A1. Every two points $P \neq Q$ are contained in a unique line ℓ .

A2. For every $P \notin \ell$ there is a unique line ℓ' on P , disjoint from ℓ .

A3. There are 3 points not on any one line.

Ignoring trivial special cases, we note by way of proof: In A1, the unique line on (x_1, y_1) , (x_2, y_2) with $x_1 \neq x_2$ is $\ell[m, k]$, where m is the unique solution of $m(x_2 - x_1) = (y_2 - y_1)$, provided by R2, and $k = -mx_1 + y_1$. In A2, for $(x_0, y_0) \notin \ell[m, k]$, the unique line ℓ' is $\ell[m, -mx_0 + y_0]$. Here we must know that every line $\ell[m, k]$ cuts every line $\ell[m', k']$ with $m' \neq m$; this follows from C3. In A3, the points $(0, 0)$, $(0, a)$, $(a, 0)$ with $a \neq 0$ ($N \geq 2$) will serve.

The plane $\pi(R)$ also satisfies the "weak" Desargues axiom, for which Artin's form [2] reads

A4. For every $P \neq Q$, there is a translation T such that $T(P) = Q$.

Here, a translation T (not the identity) means a one-one map of π to π , with no fixed point, such that, for every $P \neq Q$, the line on $T(P)$, $T(Q)$ is parallel (identical or disjoint) with that on P, Q . In our case, the general translation is $T(x, y) = (x+a, y+b)$. We note in verifying A4 (the rest being obvious) that the unique lines on $P = (x_1, y_1)$, $Q = (x_2, y_2)$, $x_1 \neq x_2$, and on $T(P)$, $T(Q)$, are $\ell[m, k]$, $\ell[m, -ma+k+b]$, as determined by A1. Two such lines

with the same m are parallel.

Although it follows from geometric considerations, it may be of interest to state as a "ring theoretic" result

Theorem 1. Every finite group $R, +$, of order $N \geq 2$, with a product satisfying R1, R2, is Abelian, indeed a vector space of order $N = p^n$ and dimension n over a Galois field $GF(p)$, $p \geq 2$, $n \geq 1$.

Proof. (a) To show $a + b \equiv b + a$, we may suppose $a \neq 0$. By R2, there is a unique m such that $ma = a$, and a unique m' such that $m'a = b + a - b$. The result follows if $m = m'$. If $m \neq m'$, there is a unique x_0 such that $mx_0 = m'x_0 + b$, by C3. But then $m(x_0 + a) = mx_0 + a$, and also $m'(x_0 + a) + b = m'x_0 + m'a + b = m'x_0 + b + a = mx_0 + a$, whence $x_0 + a = x_0$ (by the uniqueness italicized) and $a = 0$, a contradiction.

(b) Knowing that $R, +$ is Abelian, we may introduce its endomorphism ring Ω , which contains for each (left multiplier) x an operator $X = X(x)$ such that $Xy \equiv xy$ (cf. R1). Let Γ be the set of all $C \in \Omega$ for which a $D \in \Omega$ exists such that $XC \equiv DX$ for all $X(x)$. We contend that Γ is a (finite) field, hence a Galois field $GF(p^t)$. The ring properties of Γ are immediate; we need only show that every $C \neq 0$ is one-one on R . Suppose then that $Cx_1 \neq 0$ for some x_1 , but $Cx_0 = 0$ for an $x_0 \neq 0$. Then for all $X(x)$ we should have $0 \equiv XCx_0 \equiv DXx_0$. Since $x_0 \neq 0$, Xx_0 ranges over all of R by R2. But then $D = 0$ and $KCx_1 \equiv DXx_1 \equiv 0$, for all $X(x)$, whereas (since $Cx_1 \neq 0$) there is an X_1 such that $X_1(Cx_1) = Cx_1 \neq 0$, by R2.

(c) Since the identity I of Ω is in $\Gamma \cong GF(p^t)$, we must have, for p summands, $0 = 0x = (I + \dots + I)x = Ix + \dots + Ix = x + \dots + x$. Thus every x is of "height" p , and the Abelian group $R, +$ is a vector space of order $N = p^n$ over $GF(p)$.

We may therefore regard the elements of $R, +$ as column vectors $x = [\xi_i]$, and the ring Ω as consisting of all $n \times n$ matrices $M = [\mu_{ij}]$, $\xi_i, \mu_{ij} \in GF(p)$. We are thus led to

Theorem 2. If $R, +$ is a vector space over $GF(p)$, of order $N = p^n$, the definition of a product satisfying R1, R2 is equivalent to the production of a

set $I = \{X_1, \dots, X_N\}$ of matrices in Ω with the property:

(Δ) the difference of every two matrices of the set is nonsingular.

Proof. (a) Given such a product, each $x \in R$ defines by R1 a unique matrix $X(x)$ such that $xy \equiv X(x)y$. If $X(x) - X(y)$ were singular, we should have $xz \equiv X(x)z = Y(x)z \equiv yz$ for some $z \neq 0$, and $x = y$ by R2.

(b) If a Δ -set $I = \{X\}$ is given, we may set up an arbitrary one-one map $x \rightarrow X(x)$ on R to I and define $xy \equiv X(x)y$. Then R1 is a property of matrices, and R2 follows from the nonsingular difference property (Δ).

We next show that the general systems R of Theorem 1 are related in a simple and definite way to a "canonical" system in which

$$R3. 0x \equiv 0 \equiv x0$$

$$R4. ex \equiv x \equiv xe \text{ for some } e \text{ of } R.$$

A vector space $R, +$ of order $N = p^n$ over $GF(p)$ with a product satisfying R1-R4 is called a Veblen-Wedderburn (V-W) system.

If 0 is not in the Δ -set $I = \{X_i\}$ of a system R , then it is in the Δ -set $I' = \{X_i - X_1\}$; making the assignment $X'(0) = 0$ in the correspondence $x \rightarrow X'(x)$ yields a system R' in which $0x \equiv 0 \equiv x0$. In R' , we have R2'. $x \rightarrow zx$ is one-one for $z \neq 0$. Now, if I is not in I' , it is in the Δ -set

$$I'' = \{(X_1 - X_1)(X_2 - X_1)^{-1}\}.$$

If we select an arbitrary $e \neq 0$ from R' and stipulate $X''(e) = I$ as well as $X''(0) = 0$, we see that $0x \equiv 0 \equiv x0$ and $ex \equiv x$. If we completely specify the correspondence $x \rightarrow X''(x)$ by the identity $X''(x)e \equiv x$, it is clear that the corresponding system R'' satisfies R3 and R4. Such a specification is possible, since Xe with $e \neq 0$ ranges over all x as X ranges over any Δ -set.

It may be shown that, although these systems R, R', R'' are in general nonisomorphic, the corresponding planes are isomorphic geometrically. Moreover, it is well-known [3] that every plane $A1-A4a$ is isomorphic to a plane $\pi(R)$, where R is a V-W system [3]. We lose nothing, algebraically or geometrically, by considering in the sequel the V-W systems R1-R4.

For the Δ -set $I = \{0, I, X_2, \dots, X_N\}$ of such a system, the field Γ is the commutator in Ω of I ,

i.e., $\Gamma = \{C; CX \equiv XC\}$.

If a V-W system R satisfies the remaining distributive law

$$(D) \quad (x+y)z = xz + yz,$$

it is a "division algebra"; if, moreover, $x(yz) = (xy)z$, it is a finite field $GF(p^n)$. The set χ is then the "regular representation" of R, with $X(x+y) = X(x) + X(y)$, $X(xy) = X(x)X(y)$, and $\Gamma \equiv \chi$. The plane $\pi(R)$ then (and only then) satisfies the "strong" axiom of Desargues [2,3].

2. V-W Systems from $GF(p^n)$. For every p and n there exists an irreducible polynomial $m(\lambda) = \lambda^n - \alpha_{n-1}\lambda^{n-1} - \dots - \alpha_0$ of degree n over $GF(p)$. If the $N = p^n$ formal elements $x = \xi_0 + \xi_1 r + \dots + \xi_{n-1} r^{n-1}$, $\xi_i \in GF(p)$, be added as coefficients, and multiplied as formal polynomials in r, subject to the reduction $r^n = \alpha_0 + \alpha_1 r + \dots + \alpha_{n-1} r^{n-1}$, one obtains a realization of the Galois field $F = GF(p^n)$. This has exactly n $GF(p)$ -automorphisms

$$x \rightarrow \theta_a(x) = x^{p^a}, \quad a = 1, 2, \dots, n,$$

θ_n being the identity. The $(\cdot)$ group of F is cyclic, with a generator g of period $p^n - 1$ [6]. By using automorphisms to deform the multiplication in F, one may produce a variety of V-W systems, as indicated in

Theorem 3. There exists a V-W system not satisfying the law (D) for every $p \geq 2$, $n \geq 2$ with p odd, and for $p = 2$ with n composite.

Proof. Let d be an integer such that

$1 < d | p^n - 1$. To each $j = 1, \dots, d$ assign an integer $a(j)$ on $\{1, \dots, n\}$ such that

- (1) $d | p^{a(j)} - 1$ for each $a = a(j)$
- (2) $a(d) = n$
- (3) $a(j) < n$ for at least one $j < d$.

This is always possible for p odd (say $d = 2$), and for $p = 2$ if, and only if, n is composite (if $n = ab$, $a, b > 1$, set $d = 2^a - 1$). Note that the g.c.d. $(2^a - 1, 2^n - 1) = 2^c - 1$ where $c = (a, n)$ [4]. For $1 \leq a < n$, $2^c - 1 = 1$ regardless of the primality of $2^n - 1$.

On the elements of $F = GF(p^n)$, define $(+)$ as

in F, and a product $x \cdot y$ by

$$M1. \quad 0 \cdot x = 0$$

$$M2. \quad \text{for } 0 \neq \xi = g^J, J \equiv j \pmod{d}, 1 \leq j \leq d, \\ a = a(j), A = p^a \text{ set } x \cdot y = xy^A.$$

The right side, referring to $(\cdot)$ in F, is well-defined, since $J \equiv J' \pmod{p^n - 1}$ implies $J' \equiv J \equiv j \pmod{d}$.

The V-W axioms R1-R4 are easily verified, remembering that $x \rightarrow x^A$, $A = p^a$, is an automorphism. We include only a proof of R2. Suppose $x \cdot z = y \cdot z$, where $0 \neq z = g^L$. If x or y is zero, then by M1, M2, so is the other, and we assume

$$0 \neq x = g^J, J \equiv j \pmod{d}, a = a(j), A = p^a$$

$$0 \neq y = g^K, K \equiv k \pmod{d}, b = a(k), B = p^b \\ 1 \leq j, k \leq d.$$

Then $g^J g^{LA} = g^K g^{LB}$, $J + L(A-1) \equiv K + L(B-1) \pmod{p^n - 1}$, hence mod d. Since $d | A-1, B-1$ by (1), we have $j \equiv J \equiv K \equiv k \pmod{d}$, and $j = k$, $a = b$, $A = B$, so that $x = g^J = g^K = y$.

To see that (D) fails, we follow an argument of André [1]. Consider an element g^j with $a = a(j) < n$ as in (3), and set $A = p^a < p^n$. Clearly $g^j \neq 1 = g^{p^n - 1}$, so $0 \neq g^j - 1 = g^K$, $K \equiv k \pmod{d}$, $b = a(k)$, $B = p^b$. Supposing (D) true, we have $0 = 0 \cdot y = (-x+x) \cdot y = (-x) \cdot y + x \cdot y$ and $(-x) \cdot y = -(x \cdot y)$, the analogue of C2. We could then write $(g^j - 1)y^B = (g^j - 1) \cdot y = g^j \cdot y - y$, whence

$$y^B = \frac{g^j \cdot y - y}{g^j - 1} \quad \text{for all } y.$$

$$\text{Therefore } \left(\frac{g^j \cdot y - y}{g^j - 1} \right)^2 = (y^B)^2 = (y^2)^B = \frac{g^j y^{2A} - y^2}{g^j - 1}$$

which leads at once to $y^{A-1} = 1$ for all $y \neq 0$. If $y = g$, this implies $p^n - 1 | p^a - 1$, a contradiction.

Example 1. Let $p = 3$, $n = 2$, $m(\lambda) = \lambda^2 - \lambda - 1$ (irreducible over $GF(3)$), $r^2 = 1 + r$, $d = 2$, $a(1) = 1$, $a(2) = 2$. Since $r^3 = 1 - r$, $r^4 = -1$, $r^5 = -r$, $r^6 = -1 - r$, $r^7 = -1 + r$, $r^8 = 1$, r generates the $(\cdot)$ group of $GF(3^2)$. The construction indicates that $r^J \cdot r^K$ is r^{J+K} for J even, and $r^J(r^K)^3$ for J odd. Since $(r^K)^3 = r^3, r^6, r, r^4, r^7, r^2, r^5, r^8$, we obtain the $(\cdot)$ table (showing only exponents of r)

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

TABLE I. (K_7)

One may prove $x(yz) = (xy)z$ from the definition of ($\cdot$).

3. A General Method. If we represent the elements $x = \xi_0 + \dots + \xi_{n-1}r^{n-1}$ of $F = GF(p^n)$ as column vectors $x = [\xi_1]$, it is apparent that the matrix $R(x)$ defined by $xy = Ry$ is the ordinary regular representation of F by matrices in Ω . As y runs through the "1-spot" column vectors $\delta_1, \dots, \delta_n$, which represent $1, r, \dots, r^{n-1}$, the columns of $R(x)$ are produced. The Δ -set of F consists of the $R(x)$, where note $R(x)\delta_1 = x$.

The automorphism method of §2, defining $x \cdot y = xy^A$ for suitable A , yields a V-W system with a Δ -set of matrices $R(x)A(x)$, where $A(x)y \equiv y^A$; i.e., $A(x)$ is the matrix inducing the automorphism in question.

This suggests a general method of searching for V-W systems. An arbitrary Δ -set may be written in the form $L = \{R(x)A(x)\}$, with $R(x)$ as above, and $A(x)$ nonsingular. Since $R(0) = 0$, we require only that $R(x)A(x)$ for $x \neq 0$ shall form a Δ -set; equivalently, that $x \rightarrow R(x)A(x)y$ be one-one. Since $R(1) = I$ and $X(1) \equiv R(1)A(1) = I$ is stipulated, $A(1) = I$ is mandatory. Also, since $R(x)A(x)\delta_1 \equiv x$ is required, we must have $R(x)a_1 \equiv x$ where a_1 is the first column of $A(x)$. But the vector x is already the first of the linearly independent columns of $R(x)$. Hence, $a_1 = \delta_1$, and the candidates for the $A(x)$ are all nonsingular matrices A with first column δ_1 .

We indicate the method with the field $F = GF(3^2)$ of Example 1.

The vectors $x = r^J$ and matrices $R_J = R(r^J)$ for $x \in F$ are indicated by

J	1	2	3	4	5	6	7	8
r^J	0	1	1	-1	0	-1	-1	1
	1	1	-1	0	-1	-1	1	0
R_J	0 1	1 1	1 -1	-1 0	0 -1	-1 -1	-1 1	1 0
	1 1	1 -1	-1 0	0 -1	-1 -1	-1 1	1 0	0 1

The first column of R_J is r^J , the second is r^{J+1} .

All the nonsingular matrices A with $a_1 = \delta_1$ are

K	1	2	3	4	5	6
A_K	1 0	1 0	1 1	1 1	1 -1	1 -1
	0 1	0 -1	0 1	0 -1	0 1	0 -1

The following table shows their action on the vectors r^L in terms of L :

A_1	1	2	3	4	5	6	7	8
A_2	5	3	2	4	1	7	6	8
A_3	2	7	5	4	6	3	1	8
A_4	3	6	1	4	7	2	5	8
A_5	7	1	6	4	3	5	2	8
A_6	6	5	7	4	2	1	3	8

The action of the R_J on r^L is indicated in the cyclic table

R_1	2	3	4	5	6	7	8	1
R_2	3	4	5	6	7	8	1	2
R_3	4	5	6	7	8	1	2	3
R_4	5	6	7	8	1	2	3	4
R_5	6	7	8	1	2	3	4	5
R_6	7	8	1	2	3	4	5	6
R_7	8	1	2	3	4	5	6	7
R_8	1	2	3	4	5	6	7	8

TABLE II. (K_1)

Iteration shows the action on the r^L of the operators $R_{J,K}$, for each $J = 1, \dots, 7$, and all $K = 1, \dots, 6$. For example one finds for R_1 the results

R_{1A_1}	2	3	4	5	6	7	8	1
R_{1A_2}	6	4	③	5	2	8	7	1
R_{1A_3}	3	8	6	5	7	4	2	1
R_{1A_4}	4	7	2	5	8	3	6	1
R_{1A_5}	8	②	7	5	4	6	3	1
R_{1A_6}	7	6	8	5	3	2	4	1

Discarding those pairs $R_{J,K}$ which result in a conflict with the normal order $1, \dots, 8$ defined by the pair $R_{8A_1} = I$, we find in this way the possibilities (J,K) listed:

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

Systematic search for choice functions $K = K(J)$, resulting in a multiplication table $R_{J,K(J)} \cdot r^L$ with no repetition in any column reveals the following 12 possibilities

J	K(J)											
J	K_1	K_2	K_3	K_4	K_5	K_6	K_7	K_8	K_9	K_{10}	K_{11}	K_{12}
1	1	1	1	3	3	3	4	4	4	6	6	6
2	1	3	6	2	3	6	1	2	2	1	3	6
3	1	2	1	5	2	4	4	2	5	1	5	4
4	1	5	1	1	3	1	1	3	1	3	5	5
5	1	1	3	1	3	3	4	2	4	2	4	2
6	1	1	2	6	5	6	1	2	2	5	5	6
7	1	6	5	1	4	4	4	6	5	1	5	6
8	1	1	1	1	1	1	1	1	1	1	1	1

A study of the corresponding 12 multiplication tables shows that there are just five nonisomorphic V-W systems of order 3^2 :

For $i = 1, 6, 9$ the K_i define $F = GF(3^2)$. Table II is the result for K_1 . The mappings $L \rightarrow \theta(L)$ establishing the $(+, \cdot)$ -isomorphism here are

K_1	1	2	3	4	5	6	7	8
K_6	2	7	5	4	6	3	1	8
K_9	6	5	7	4	2	1	3	8

The remaining nine systems all violate the law (D).

For $i = 2, 5, 8, 10, 11, 12$, the K_i define isomorphic systems. Table III shows the $(\cdot)$ for K_2 . The isomorphisms may be defined as follows

K_2	1	2	3	4	5	6	7	8
K_5	5	3	2	4	1	7	6	8
K_8	6	5	7	4	2	1	3	8
K_{10}	3	6	1	4	7	2	5	8
K_{11}	7	1	6	4	3	5	2	8
K_{12}	2	7	5	4	6	3	1	8

A glance at the main diagonals of Tables III, IV, V, and I shows that the corresponding systems, defined by K_2, K_3, K_4 , and K_7 , respectively, are all non-isomorphic, except possibly those for K_3, K_4 . In Table IV one sees that $x \equiv r$ has the property $(x \cdot x) \cdot x = r^8$ (identity). No nonidentity element has this property in Table V. The system defined by K_7 is of course the one in Example 1.

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

TABLE III. (K_2) TABLE IV. (K_3) TABLE V. (K_4)

The method is still within the reach of hand computation for $p = 2$, $n = 3$, and of course shows that there are no V-W systems of order 2^3 except $GF(2^3)$ [5]. It is an open question whether (for r prime) all V-W systems of order 2^r are fields $GF(2^r)$. The case $r = 5$ seems within the range of a machine attack.

REFERENCES

1. J. André, "Über nicht-Desarguessche Ebenen mit Transitiver Translationsgruppe," *Math. Z.* 60, 156-186 (1954). See p. 185.
2. E. Artin, *Geometric Algebra*, Interscience Publishers, N.Y., 1957, pp. 58, 70.
3. R. H. Bruck, "Recent Advances in the Foundations of Euclidean Plane Geometry," *Am. Math. Monthly* 62, Part II, 2-17 (1955).
4. E. D. Cashwell and C. J. Everett, "Fibonacci Spaces," *Fibonacci Quarterly* 4, 97-115 (1966).
5. M. Hall, Jr., "Numerical Analysis of Finite Geometries," *Proceedings of the IBM Scientific Symposium on Combinatorial Problems*, 1964, pp. 11-22.
6. C. C. MacDuffee, *Introduction to Abstract Algebra*, Wiley, N.Y., 1940, p. 174.