ON SOME TACTICAL CONFIGURATIONS

HAIM HANANI

1. Introduction. Given a set E of v elements, and given positive integers k, l $(l \leqslant k \leqslant v)$, and λ, we understand by a *tactical configuration* $C[k, l, \lambda, v]$ (briefly, *configuration*) a system of subsets of E, having k elements each, such that every subset of E having l elements is contained in exactly λ sets of the system.

A necessary condition for the existence of a configuration $C[k, l, \lambda, v]$ is known **(6)** to be

$$\text{(i)} \qquad \lambda\cdot\binom{v-h}{l-h}\Big/\binom{k-h}{l-h} = \text{integer}, \qquad h = 0, 1, \ldots, l-1.$$

The problem of determining the values of k, l, and λ for which this condition is also sufficient is not yet solved completely.

Configurations with $l = 2$ are known as balanced incomplete block designs (BIBD). It has been proved by Reiss **(9)** and Moore **(7)** that for BIBD with $k = 3$, $\lambda = 1$ (known also as the Steiner triple systems) Condition (i) is sufficient. Bose **(2)** proved sufficiency of (i) for BIBD with $k = 3$, $\lambda = 2$, and the author **(6)** for BIBD with $k = 3$ and 4 (and every λ) and $k = 5$, $\lambda = 1$, 4, and 20. On the other hand, Tarry **(11)** proved that Condition (i) is not sufficient for BIBD with $k = 6$, $\lambda = 1$; Nandi **(8)** for BIBD with $k = 5$, $\lambda = 2$; and Shrikhande **(10)** and Hall and Connor **(4)** proved the non-sufficiency of (i) for more general classes of BIBD.

Less is known about configurations with $l > 2$. The only general result so far known is **(5)** that Condition (i) is sufficient for $k = 4$, $l = 3$, $\lambda = 1$. We shall prove in this paper the sufficiency of (i) for $k = 4$, $l = 3$, and every λ. The proof will be given by effective construction of the relevant configurations. Further, the existence of some other configurations will be proved and their construction produced.

2. P-systems. In the following we shall usually assume $l = 3$ and in order to shorten notation we shall omit the value of l. On the other hand we shall have to introduce some generalizations of the configurations introduced in Section 1. For this purpose we introduce the following definitions.

DEFINITION 1. *Let a set E having v $(v \geqslant 4)$ elements be given; further let λ be*

Received October 15, 1962. A part of this paper has been written at the Mathematics Research Center, United States Army, Madison, Wisconsin, sponsored by the United States Army, under Contract No. Da-11-022-ORD-2059.

a positive integer and $K = \{k_i\}^n{}_{i=1}$ *be a finite set of integers* $k_i \geqslant 4$ $(i = 1, 2, \ldots, n)$. *If it is possible to form a system of blocks (subsets of* E*) in such a way that*

(i) *the number of elements in each block is some* $k_i \in K$ *and*

(ii) *every triple of elements of* E *is contained in exactly* λ *blocks, then we shall denote such a system by* $P[K, \lambda, v]$.

It is sometimes necessary to point out that a system $P[K, \lambda, v]$ is constructed on a given set E. In such a case we shall denote the system by $P[K, \lambda, v(E)]$.

DEFINITION 2. *Let a set* E *of* $v = mt + r$ *elements be given. We split it into* $t + 1$ *disjoint subsets, viz.* t *sets* E_i $(i = 1, 2, \ldots, t)$ *of* m *elements each, and a set* E_{t+1} *of* r *elements, and denote* $E_i' = E_i \cup E_{t+1}$ $(i = 1, 2, \ldots, t)$. *If there exists a system* $P^* = P[K, \lambda, v(E)]$ *such that* $P[K, \lambda, (m + r)(E_i')] \subset P^*$ *and if for* $r > 2$ *also* $P[K, \lambda, r(E_{t+1})] \subset P[K, \lambda, (m + r)(E_i')]$ $(i = 1, 2, \ldots, t)$, *then the system* P^* *will be denoted by* $P_m[K, \lambda, v]$.

It is easily seen that

$$P_m[K, \lambda, v] = \bigcup_{i=1}^{t} P[K, \lambda, (m + r)(E_i')] \cup P_m'[K, \lambda, v]$$

where $P_m'[K, \lambda, v]$ is a subsystem of $P_m[K, \lambda, v]$ consisting of exactly all those blocks which have no more than two elements in common with each of the sets E_i' $(i = 1, 2, \ldots, t)$.

DEFINITION 3. *Let a set* E *of* $v = mt$ *elements be a union of its* t *disjoint subsets* E_i $(i = 1, 2, \ldots, t)$ *each having* m *elements; let* λ *be a positive integer and* $K = \{k_i\}^n{}_{i=1}$ *be a finite set of integers* $k_i \geqslant 4$ $(i = 1, 2, \ldots, n)$. *If it is possible to form a system of blocks in such a way that*

(i) *the number of elements in each block is some* $k_i \in K$,

(ii) *each block has at most one element in common with each of the sets* E_i $(i = 1, 2, \ldots, t)$, *and*

(iii) *every triple of elements of* E *having at most one element in common with each of the sets* E_i *is contained in exactly* λ *blocks,*

then we shall denote such a system by $P_m''[K, \lambda, v]$.

DEFINITION 4. *The class of integers* v *for which systems* $P[K, \lambda, v]$ *exist will be denoted by* $P(K, \lambda)$.

The classes $P_m(K, \lambda)$, $P_m'(K, \lambda)$, and $P_m''(K, \lambda)$ are defined in a similar way.

Remark 1. If $K = \{k\}$ consists of one element only, we shall write $P(k, \lambda)$ instead of $P(\{k\}, \lambda)$ and similarly $P_m(k, \lambda)$, $P_m'(k, \lambda)$, $P[k, \lambda, v]$, etc.

Remark 2. The systems $P[k, \lambda, v]$ are tactical configurations $C[k, 3, \lambda, v]$ introduced in Section 1.

Remark 3. From Definition 2 it follows that no system of the form $P_m[K, \lambda, mt + 3]$ with $t > 1$ can exist.

The following propositions may be accepted without proof.

PROPOSITION 1. *$P_m(K, \lambda) \subset P(K, \lambda)$ for every m.*

PROPOSITION 2. *$k \in P(K, 1)$ and $k \in P_1''(K, 1)$ for every $k \in K$.*

PROPOSITION 3. *If $K' \subset K$ and λ' divides λ, then $P(K', \lambda') \subset P(K, \lambda)$ and similarly $P_m(K', \lambda') \subset P_m(K, \lambda)$, $P_m'(K', \lambda') \subset P_m'(K, \lambda)$, and*

$$P_m''(K', \lambda') \subset P_m''(K, \lambda).$$

PROPOSITION 4. *If $v \in P(K', \lambda')$ and if $k' \in P(K, \lambda'')$ for every $k' \in K'$, then $v \in P(K, \lambda)$, where $\lambda = \lambda'\lambda''$.*

We shall now prove several less evident propositions.

PROPOSITION 5. *If m' divides m and if $m't \in P_{m'}''(4, \lambda')$, then $mt \in P_m''(4, \lambda)$.*

Proof. Let $m = m'm''$. Denote by (j, h) $(0 \leqslant j \leqslant m' - 1, 0 \leqslant h \leqslant t - 1)$ the jth element of the set E_h (see Definition 3). The blocks of $P_{m'}''[4, \lambda, m't]$ are of the form

$$\{(j_i, h_i) : i = 0, 1, 2, 3; 0 \leqslant j_i \leqslant m' - 1; 0 \leqslant h_i \leqslant t - 1; h_i \neq h_{i'} \text{ for } i \neq i'\}.$$

From each such block construct $(m'')^3$ blocks as follows:

$$\left\{(j_i + a_i m', h_i) : 0 \leqslant a_i \leqslant m'' - 1; \sum_{i=0}^{3} a_i \equiv 0 \pmod{m''}\right\}.$$

It can be easily verified that the blocks thus constructed form a $P_m''[4, \lambda, mt]$.

PROPOSITION 6. *If $v = 2t$ where $t \in P(K', \lambda')$ and if for every $k' \in K'$, $2k' \in P_2''(K, \lambda'')$ holds, and moreover $4 \in K$, then $v \in P(K, \lambda)$ where $\lambda = \lambda'\lambda''$.*

Proof. Let us denote the elements of a set E having v elements by (i, j) $(i = 0, 1; j = 0, 1, \ldots, t - 1)$. The blocks of $P[K, \lambda, v]$ are constructed as follows: for every pair j, j' $(0 \leqslant j, j' \leqslant t - 1, j' \neq j)$ take λ times the quadruple $\{(0, j), (1, j), (0, j'), (1, j')\}$. Further for every block $\beta \in P[K', \lambda', t]$ on the set $\{j\}_{j=0}^{t-1}$ construct the system $P_2''[K, \lambda'', 2|\beta|]$ on the set $\{(i, j) : i = 0, 1; j \in \beta\}$. Here $|\beta|$ denotes the number of elements in β.

PROPOSITION 7. *If $v = 2t$ where $t + 1 \in P(K', \lambda')$ and if $2(k' - 1) \in P(K, \lambda'')$ and $2k' \in P_2''(K, \lambda'')$ for every $k' \in K'$, then $v \in P(K, \lambda)$ where $\lambda = \lambda'\lambda''$.*

Proof. Denote the v elements by (i, j) $(i = 0, 1; j = 0, 1, \ldots, t - 1)$. The blocks of $P[K, \lambda, v]$ are constructed as follows. Consider the set of integers $\{j\}^t{}_{j=0}$ and construct on them a system $P[K', \lambda', t + 1]$. For every block

$\beta' \in P[K', \lambda', t+1]$ which contains the element t, omit t and construct a system $P[K, \lambda'', 2(|\beta'| - 1)]$ on the elements (i, j) $(i = 0, 1; j \in \beta' - \{t\})$. For every block $\beta \in P[K', \lambda', t+1]$ which does not contain the element t, construct a system $P_2''[K, \lambda'', 2|\beta|]$ on the elements (i, j) $(i = 0, 1; j \in \beta)$.

PROPOSITION 8. *If $v = mt + r$ where $t + 1 \in P(K', \lambda')$ and if*

$$m(k' - 1) + r \in P_m(K, \lambda'')$$

and $mk' \in P_m''(K, \lambda'')$ for every $k' \in K'$, then $v \in P_m(K, \lambda)$ where $\lambda = \lambda'\lambda''$.

Proof. Denote the v elements by (i, j) $(i = 0, 1, \ldots, m-1; j = 0, 1, \ldots, t-1)$ and (A, s) $(s = 0, 1, \ldots, r-1)$. The blocks are as follows. On each of the sets

$$E_j' = \{(A, s), (i, j) : i = 0, 1, \ldots, m-1; s = 0, 1, \ldots, r-1\} \qquad (j = 0, 1, \ldots, t-1)$$

construct a system $P[K, \lambda'', (m + r)(E_j')]$ and take these systems λ' times each. If, however, $r > 2$ and according to Definition 2 there exists a subsystem $P[K, \lambda'', r(\{(A, s)\}_{s=0}^{r-1})]$ included in $P[K, \lambda'', (m+r)(E_j')]$ for every j, then take this subsystem and all the remainders

$$P[K, \lambda'', (m+r)(E_j')] - P[K, \lambda'', r] \qquad (j = 0, 1, \ldots . t-1),$$

λ' times each. Further construct a system $P[K', \lambda', t+1]$ on the set $\{j\}^t{}_{j=0}$; for every block β' of this system which contains the element t, omit t, and construct a system $P_m'[K, \lambda'', m(|\beta'| - 1) + r]$ on the elements (i, j) $(i = 0, 1, \ldots, m-1; j \in \beta' - \{t\})$ and (A, s) $(s = 0, 1, \ldots, r-1)$, and for every block $\beta \in P[K', \lambda', t+1]$ which does not contain the element t, construct a system $P_m''[K, \lambda'', m\,|\beta|]$ on the elements (i, j) $(i = 0, 1, \ldots, m-1; j \in \beta)$.

The next problem will be to find conditions under which

$$v = mt + r \in P(K, \lambda)$$

if $t + 2 \in P(K', \lambda')$ for some given K' and λ'. For this purpose we introduce the following definition.

DEFINITION 5. *Let a set E of $v = mt + r$ elements be subdivided into subsets E_i and E_i' as in Definition 2. Denote by T_1 the system of all those triples which have at most one element in common with each of the sets E_i and by T_2 the system of all those triples which have exactly two elements in common with at least one of the sets E_i', each triple taken λ times (where λ is a positive integer). Subdivide the system T_2 into two disjoint classes T_2' and T_2'' in such a way that all the triples which have an element in E_{t+1} belong to T_2' and that the classes T_2' and T_2'' are invariant with respect to any permutation of the sets E_i; otherwise the subdivision is arbitrary.*

Let $K = \{k_i\}^n{}_{i=1}$ *be a finite set of integers* $k_i \geqslant 4$. *If it is possible to form on* E *two systems of blocks in such a way that*

(i) *the number of elements in each block is some* $k_i \in K$, *and*

(ii) *the triples occurring in the blocks of the first system are exactly those of* $T_1 \cup T_2'$ *and in the blocks of the second system those of* $T_1 \cup T_2''$,

then we denote such systems by $Q_m'[K, \lambda, v]$ *and* $Q_m''[K, \lambda, mt]$ *respectively.*

Remark 4. The systems $Q_m'[K, \lambda, v]$ and $Q_m''[K, \lambda, mt]$ depend on the way in which the classes T_2' and T_2'' have been chosen.

Remark 5. Definition 4, Remark 1, and Proposition 3 apply also to the systems $Q_m'[K, \lambda, v]$ and $Q_m''[K, \lambda, mt]$.

PROPOSITION 9. *Suppose* $v = mt + r$ *where* $t + 2 \in P(K', \lambda')$ *and*

$$m(k' - 2) + r \in P(K, \lambda'')$$

for every $k' \in K'$. *Let* $r \in P(K, \lambda'')$ *and* $P[K, \lambda'', r] \subset P[K, \lambda'', m(k'-2) + r]$ *if* $r > 2$. *Finally, let* $mk' \in P_m''(K, \lambda'')$ *and* $m(k' - 1) + r \in Q_m'(K, \lambda'')$ *and* $m(k' - 1) \in Q_m''(K, \lambda'')$ *for suitably chosen classes* T_2', T_2'' (*see Definition* 5 *and Remark* 4). *Then* $v \in P(K, \lambda)$, *where* $\lambda = \lambda'\lambda''$.

Proof. Denote the v elements by (i, j) $(i = 0, 1, \ldots, m - 1; j = 0, 1, \ldots, t - 1)$ and (A, s) $(s = 0, 1, \ldots, r - 1)$. The blocks are constructed as follows. Form a system $P[K', \lambda', t + 2]$ on the set $\{j, x', x'' : j = 0, 1, \ldots, t - 1\}$. For every block β^* of this system which contains both the elements x' and x'' omit these elements and construct a system $P^* = P[K, \lambda'', m(|\beta^*|-2) + r]$ on the elements (i, j) $(i = 0, 1, \ldots, m - 1; j \in \beta^* - \{x', x''\})$ and (A, s) $(s = 0, 1, \ldots, r - 1)$. However, if $r > 2$, take the system $P[K, \lambda'', r]$ λ' times and instead of P^* take $P^* - P[K, \lambda'', r(\{A, s\}_{s=0}^{r-1})$. For every block $\beta' \in P[K', \lambda', t + 2]$ which contains the element x' but not x'', construct a system $Q_m'[K, \lambda'', m(|\beta'| - 1) + r]$ on the elements (i, j) $(i = 0, 1, \ldots, m-1; j \in \beta' - \{x'\})$ and (A, s) $(s = 0, 1, \ldots, r - 1)$. For every block

$$\beta'' \in P\{K', \lambda', t + 2\}$$

which contains the element x'' but not x', construct a system

$$Q_m''[K, \lambda'', m(|\beta''| - 1)]$$

on the elements (i, j) $(i = 0, 1, \ldots, m - 1; j \in \beta'' - \{x''\})$. Finally, for every block $\beta \in P[K', \lambda', t + 2]$ which contains neither x' nor x'' construct a system $P_m''[K, \lambda'', m|\beta|]$ on the elements (i, j) $(i = 0, 1, \ldots, m - 1; j \in \beta)$.

3. Tactical configurations $C[4, 3, \lambda, v]$.

THEOREM 1. *A necessary and sufficient condition for the existence of a configuration* $C[4, 3, \lambda, v]$ *is*

(ii) $\lambda v \equiv 0 \pmod 2$, $\lambda(v-1)(v-2) \equiv 0 \pmod 3$, *and* $\lambda v(v-1)(v-2) \equiv 0 \pmod 8$.

https://doi.org/10.4153/CJM-1963-069-5 Published online by Cambridge University Press

Proof. The necessity of (ii) follows from (i), Section 1. Its sufficiency will be proved in a series of lemmas. (ii) is equivalent to a statement that a configuration $C[4, 3, \lambda, v]$ exists if

$$\begin{aligned}
&\lambda \equiv 1, 5, 7, \text{ or } 11 \pmod{12} \text{ and } v \equiv 2 \text{ or } 4 \pmod 6;\\
&\lambda \equiv 2 \text{ or } 10 \pmod{12} \text{ and } v \equiv 1, 2, 4, 5, 8, \text{ or } 10 \pmod{12};\\
&\lambda \equiv 3 \text{ or } 9 \pmod{12} \text{ and } v \equiv 0 \pmod 2;\\
&\lambda \equiv 4 \text{ or } 8 \pmod{12} \text{ and } v \equiv 1 \text{ or } 2 \pmod 3;\\
&\lambda \equiv 6 \pmod{12} \text{ and } \nu \equiv 0, 1, \text{ or } 2 \pmod 4;\\
\text{or } &\lambda \equiv 0 \pmod{12}.
\end{aligned}$$

By Proposition 3 it suffices to show that for every $v \geqslant 4$

$$\begin{array}{lll}
(\text{T}.1) & v \equiv 0 \pmod 2 & \text{implies } v \in P(4, 3),\\
(\text{T}.2) & v \equiv 4 \pmod 6 & \text{implies } v \in P(4, 1),\\
(\text{T}.3) & v \equiv 2 \pmod 6 & \text{implies } v \in P(4, 1),\\
(\text{T}.4) & v \equiv 1 \pmod 6 & \text{implies } v \in P(4, 4),\\
(\text{T}.5) & v \equiv 5 \pmod 6 & \text{implies } v \in P(4, 4),\\
(\text{T}.6) & v \equiv 1 \pmod{12} & \text{implies } v \in P(4, 2),\\
(\text{T}.7) & v \equiv 5 \pmod{12} & \text{implies } v \in P(4, 2),\\
(\text{T}.8) & v \equiv 1 \pmod 4 & \text{implies } v \in P(4, 6),\\
(\text{T}.9) & v \equiv 3 \pmod{12} & \text{implies } v \in P(4, 12).
\end{array}$$

Statements (T.1) to (T.8) will be proved by methods outlined in Section 2 and in particular (T.1) will be proved in Lemma 2, (T.2) in Lemma 3, (T.3) follows from Lemmas 4 and 11, (T.4) is proved in Lemma 6, (T.5) in Lemma 5, (T.6) in Lemma 9, (T.7) in Lemma 10, and (T.8) follows from Lemmas 7 and 8. Regarding (T.9) the methods of Section 2 do not seem to apply for reasons mentioned in Remark 3 and the proof of this part of the theorem will be given in Section 4, Lemma 13.

LEMMA 1. *If* $v \equiv 0 \pmod 2$, *then* $v \in P(\{4, 6\}, 1)$.

Proof. The proof is given by induction. For $v = 4$ the lemma is true by Proposition 2. For $v \geqslant 6$ we write $v = 2t$ and assume that either $t \in P(\{4, 6\}, 1)$ or $t + 1 \in P(\{4, 6\}, 1)$.

If $t \in P(\{4, 6\}, 1)$ we make use of Proposition 6, putting $K' = K = \{4, 6\}$, $\lambda' = \lambda'' = 1$. Accordingly it remains to be proved that $8 \in P_2''(\{4, 6\}, 1)$ and $12 \in P_2''(\{4, 6\}, 1)$.

$$8 \in P_2''(\{4, 6\}, 1) \tag{1}$$

follows by Proposition 3 from

$$8 \in P_2''(4, 1) \tag{2}$$

and this follows from Proposition 2 with $K = \{4\}$ and Proposition 5 with $\lambda = 1$, $t = 4$, $m' = 1$, $m = 2$.

https://doi.org/10.4153/CJM-1963-069-5 Published online by Cambridge University Press

To prove

(3) $$12 \in P_2''(\{4, 6\}, 1),$$

denote the elements by (i, j) $(i = 0, 1; j = 0, 1, \ldots, 5)$ and form the blocks*

$\{(i, 0), (i, 1), (i, 2), (i, 3), (i, 4), (i, 5)\}$ $\quad (i = 0, 1)$;
$\{(i, j), (i, j + 2), (i + 1, j + 1), (i + 1, j + 4)\}$ $\quad (i = 0, 1; j = 0, 1, \ldots, 5)$;
$\{(0, j), (0, j + 2), (1, j + 3), (1, j + 5)\}$;
$\{(0, 2\gamma), (0, 2\gamma + \epsilon), (1, 2\gamma'), (1, 2\gamma' + \epsilon)\}$
$(\gamma, \gamma' = 0, 1, 2; \gamma' \neq \gamma; \epsilon = \pm 1)$.

If $t + 1 \in P(\{4, 6\}, 1)$, it suffices to prove, on account of Proposition 7, that $6 \in P(\{4, 6\}, 1)$, $10 \in P(\{4, 6\}, 1)$, $8 \in P_2''(\{4, 6\}, 1)$ and $12 \in P_2''(\{4, 6\}, 1)$. For the last formulas see (1) and (3) respectively; the first one follows from Proposition 2 and the second one follows by Propositions 3 and 1 from

(4) $$10 \in P_3(4, 1),$$

which will now be proved.

Elements: (i, j) $\quad (i = 0, 1, 2; j = 0, 1, 2)$ and (A).
Blocks: $\{(A), (0, j), (1, j), (2, j)\}$ $\quad (j = 0, 1, 2)$;
$\{(A), (i, 0), (i + \gamma, 1), (i + 2\gamma, 2)\}$ $\quad (i = 0, 1, 2; \gamma = 0, 1, 2)$;
$\{(i, j), (i, j + 1), (i + 1, j), (i + 1), j + 1)\}$;
$\{(i, j + 1), (i, j + 2), (i + 1, j), (i + 2, j)\}$.

The first set of blocks forms the systems $P[K, \lambda, (m + \mathrm{r})(E_i')]$ mentioned in Definition 2. In this case each of these systems consists of one block.

LEMMA 2. *If* $v \equiv 0 \pmod 2$, *then* $v \in P(4, 3)$.

Proof. By Proposition 4 and Lemma 1 this lemma follows from

(5) $$6 \in P(4, 3).$$

The configuration $P[4, 3, 6]$ is obtained by taking all the quadruples out of 6 elements.

LEMMA 3. *If* $v \equiv 4 \pmod 6$, *then* $v \in P(4, 1)$.

Proof. Here $v = 3t + 1$ and by Lemma 1, $t + 1 \in P(\{4, 6\}, 1)$. By Proposition 8 this lemma will follow from $10 \in P_3(4, 1)$, $16 \in P_3(4, 1)$, $12 \in P_3''(4, 1)$ and $18 \in P_3''(4, 1)$. For the first formula see (4); the others will be proved presently.

Proof of

(6) $$16 \in P_3(4, 1).$$

*All the numbers appearing in parentheses should be taken "mod" the number of values which the variable in the given place may take. In the given case the number in the first place is taken "(mod 2)" and that in the second place "(mod 6)."

https://doi.org/10.4153/CJM-1963-069-5 Published online by Cambridge University Press

Elements: (i, j) $\quad (i = 0, 1, 2; j = 0, 1, 2, 3, 4)$ *and* (A).
Blocks: $\{(A), (0, j), (1, j), (2, j)\}$;
$\{(A), (i + \alpha, j), (i, j - \alpha), (i, j + \alpha)\}$ $\quad (\alpha = 1, 2)$;
$\{(i, j), (i - \alpha, j), (i, j - \alpha), (i, j + \alpha)\}$ $\quad (\alpha = 1, 2)$;
$\{(i, j), (i + \alpha, j), (i, j + \epsilon\alpha), (i - \alpha, j - \epsilon\alpha)\}$ $\quad (\alpha = 1, 2; \epsilon = \pm 1)$;
$\{(i, j - 2), (i, j + 2), (i + 1), j - 1), (i + 1, j + 1)\}$.

The first set of blocks forms the systems $P[K, \lambda, (m + r)(E_i')]$ mentioned in Definition 2.

The relation

$$12 \in P_3''(4, 1) \tag{7}$$

follows from Propositions 2 and 5.

We finally prove

$$18 \in P_3''(4, 1). \tag{8}$$

Elements: (i, j) $\quad (i = 0, 1, 2; j = 0, 1, \ldots, 5)$.
Blocks: $\{(i, 2\gamma), (i, 2\gamma + 1), (i + \delta, 2\gamma + 2), (i + \delta, 2\gamma + 3)\}$
$(\gamma = 0, 1, 2; \delta = 0, 1, 2)$;
$\{(i, 2\gamma), (i+1, 2\gamma+1), (i+\delta, 2\gamma+\beta+2), (i-\delta+\gamma+\beta(\gamma-1), 2\gamma+\beta+4)\}$
$(\beta = 0, 1; \gamma = 0, 1, 2; \delta = 0, 1, 2)$;
$\{(i, 2\gamma), (i-1, 2\gamma+1), (i+\delta, 2\gamma+\beta+2), (i-\delta+\beta+(-1)^{\beta+\gamma}, 2\gamma-\beta+5)\}$
$(\beta = 0, 1; \gamma = 0, 1, 2; \delta = 0, 1, 2)$.

LEMMA 4. *If* $v \equiv 8 \pmod{12}$, *then* $v \in P(4, 1)$.

Proof. Put $v = 2t$. By Lemma 3, $t \in P(4, 1)$. Therefore, considering (2) the lemma follows from Proposition 6.

LEMMA 5. *If* $v \equiv 5 \pmod 6$, *then* $v \in P(4, 4)$.

Proof. Here $v = 3t + 2$ and by Lemma 1, $t + 1 \in P(\{4, 6\}, 1)$. By Proposition 8 this lemma follows from $11 \in P_3(4, 4)$, $17 \in P_3(4, 4)$, $12 \in P_3''(4,4)$, and $18 \in P_3''(4, 4)$. The last two formulas follow from (7) and (8) respectively and from Proposition 3. The other will be now proved. We first prove

$$11 \in P_3(4, 4). \tag{9}$$

Elements: (i, j) $\quad (i = 0, 1, 2; j = 0, 1, 2)$ and (A, s) $\quad (s = 0, 1)$.
Blocks: Form all the quadruples on the sets $\{(A, s), (i, j): s = 0, 1; i = 0, 1, 2\}$ and take them twice. These are the systems $P[4, 4, 5(E_j')]$ $(j = 0, 1, 2)$ mentioned in Definition 2. Further construct the blocks of $P_3'[4, 4, 11]$ as follows:

$\{(A, s), (i_0, 0), (i_1, 1), (i_2, 2)\}$ $\quad (s = 0, 1; i_0, i_1, i_2 = 0, 1, 2$ independently$)$;

$\{(A, s), (a_0, 0), (a_1, 1), (a_2, 2)\}$ $\quad \left(s = 0, 1; \sum_{h=0}^{2} a_h \equiv 0 \pmod 3\right)$;

$\{(i, j+1), (i, j+2), (i+1, j), (i+2, j)\}$ twice;
$\{(i, j), (i, j+1), (i+1, j), (i+1, j+1)\}$ twice;
$\{(i, j), (i+1, j), (i+\gamma, j+1), (i+\gamma+1, j+1)\}$ $(\gamma = 0, 1, 2)$.

It remains to prove

$$(10) \qquad 17 \in P_3(4, 4).$$

Elements: (i, j) $(i = 0, 1, 2; j = 0, 1, 2, 3, 4)$ and (A, s) $(s = 0, 1)$.
Blocks: Form the blocks $P[4, 4, 5(E_j')]$ as in the proof of (9), but here $j = 0, 1, 2, 3, 4$. Further construct the blocks of $P_3'[4, 4, 17]$ as follows:

$$\{(A, s), (a_0, j), (a_1, j-\alpha), (a_2, j+\alpha)\}$$

$$\left(\sum_{h=0}^{2} a_h \equiv s + 1 \pmod 3, s = 0, 1; \alpha = 1, 2\right);$$

$\{(A, s), (i+s+1, j), (i, j-\alpha), (i, j+\alpha)\}$ $(\alpha = 1, 2)$;
$\{(i, j), (i+1, j), (i+\beta, j-\epsilon\alpha), (i+2, j+\epsilon\alpha)\}$ $(\alpha = 1, 2; \beta = 0, 1; \epsilon = \pm 1)$;

$$\{(a_0, j), (a_1, j+1), (a_2, j+2), (a_3, j+3)\} \qquad \left(\sum_{h=0}^{3} a_h \equiv 0 \pmod 3\right);$$

$\{(i, j), (i, j+1), (i, j+2), (i, j+3)\}$;
$\{(i, j), (i+1, j), (i, j+\alpha), (i+1, j+\alpha)\}$ $(\alpha = 1, 2)$;
$\{(i, j), (i+1, j), (i+\gamma, j+\alpha), (i+\gamma+1, j+\alpha)\}$ $(\alpha = 1, 2; \gamma = 0, 1, 2)$.

LEMMA 6. *If* $v \equiv 1 \pmod 6$, *then* $v \in P(4, 4)$.

Proof. $v = 3t + 1$ and by Lemma 1, $t + 2 \in P(\{4, 6\}, 1)$. Considering Proposition 9 we have to prove $7 \in P(4, 4)$, $13 \in P(4, 4)$. Further, for suitably chosen classes T_2' and T_2'', $10 \in Q_3'(4, 4)$, $16 \in Q_3'(4, 4)$, $9 \in Q_3''(4, 4)$, $15 \in Q_3''(4, 4)$, and also $12 \in P_3''(4, 4)$, and $18 \in P_3''(4, 4)$. The last two formulas follow from (7), (8), and Proposition 3. The others will be proved.

The relation

$$(11) \qquad 7 \in P(4, 4)$$

is obtained by taking all the quadruples out of 7 elements.

By Propositions 3 and 1 the relation

$$(12) \qquad 13 \in P(4, 4)$$

follows from

$$(13) \qquad 13 \in P_4(4, 2).$$

Proof of (13). *Elements*: (i, j) $(i = 0, 1, 2, 3; j = 0, 1, 2)$ and (A).
Blocks: Form all the quadruples on the sets

$$\{(A), (i, j); i = 0, 1, 2, 3\} \qquad (j = 0, 1, 2).$$

Further construct the system $P_4'[4, 2, 13]$ as follows:

$$\{(A), (a_0, 0), (a_1, 1), (a_2, 2)\} \qquad \left(\sum_{h=0}^{2} a_h \equiv 1 \pmod 2\right);$$

$$\{(a_0, j), (a_0 + 2, j), (a_1, j + 1), (a_2, j + 2)\} \qquad \left(\sum_{h=0}^{2} a_h \equiv j \pmod 4\right);$$

$$\{(i, j), (i + 1, j), (i + \delta, j + 1), (i + \delta + 1, j + 1)\} \qquad (\delta = 0, 1, 2, 3).$$

In order to prove the other formulas we have to choose the classes T_2', T_2''. We know that every triple which appears in T_2 occurs there four times. We put every such triple which does not contain the element (A) twice in T_2' and twice in T_2''. We prove

(14) $$10 \in Q_3'(4, 4).$$

Elements: (i, j) $\quad (i = 0, 1, 2; j = 0, 1, 2)$ and (A).

Blocks: $\{(A), (a_0, 0), (a_1, 1), (a_2, 2)\} \quad \left(\sum_{h=0}^{2} a_h \equiv 0 \pmod 3\right)$

taken 4 times;

$\{(i, j + 1), (i, j + 2), (i + 1, j), (i + 2, j)\}$ twice;
$\{(i, j), (i + 1, j), (i, j - \epsilon), (i + 1, j + \epsilon)\}$ $(\epsilon = \pm 1)$;
$\{(i, j), (i, j + 1), (i + 1, j), (i + 1, j + 1)\}$.

We next prove

(15) $$16 \in Q_3'(4, 4).$$

Elements: (i, j) $\quad (i = 0, 1, 2; j = 0, 1, 2, 3, 4)$ and (A).
Blocks: $\{(A), (i, j), (i - \gamma, j - \alpha), (i + \gamma, j + \alpha)\}$ $(\alpha = 1, 2; \gamma = 0, 1, 2)$;
$\{(i, j - \alpha), (i, j + \alpha), (i + 1, j - 2\alpha), (i + 1, j + 2\alpha)\}$ $(\alpha = 1, 2)$;
$\{(i - 1, j), (i + 1, j), (i, j - \alpha), (i, j + \alpha)\}$ $(\alpha = 1, 2)$;
$\{(i, j), (i + 1, j), (i, j + \alpha), (i + 1, j + \alpha)\}$ $(\alpha = 1, 2)$;

$$\{(a_0, j), (a_1, j + 1), (a_2, j + 2), (a_3, j + 3)\} \qquad \left(\sum_{h=0}^{3} a_h \equiv 0 \pmod 3\right).$$

Further add the blocks of a system $P_3'[4, 1, 16]$ which is the system constructed in (6) without the blocks $\{(A), (0, j), (1, j), (2, j)\}$.
Proof of

(16) $$9 \in Q_3''(4, 4).$$

Elements: (i, j) $\quad (i = 0, 1, 2; j = 0, 1, 2)$.

Blocks: $\{(a_0, j), (a_0 + 1, j), (a_1, j + 1), (a_2, j + 2)\} \quad \left(\sum_{h=0}^{2} a_h \equiv j \pmod 3\right)$

taken twice.

Proof of

(17) $$15 \in Q_3''(4, 4).$$

Elements: (i, j) $(i = 0, 1, 2; j = 0, 1, 2, 3, 4)$.
Blocks: $\{(i, j), (i + 1, j), (i + \gamma, j - \alpha), (i + \gamma, j + \alpha)\}$,
$(\alpha = 1, 2; \gamma = 0, 1, 2)$;
$\{(i, j - \alpha), (i, j + \alpha), (i + 1, j - 2\alpha), (i + 1, j + 2\alpha)\}$ $(\alpha = 1, 2)$;
$\{(i, j - \alpha), (i, j + \alpha), (i - \epsilon, j - 2\alpha), (i + \epsilon, j + 2\alpha)\}$ $(\alpha = 1, 2; \epsilon = \pm 1)$;

all these blocks are taken twice.

LEMMA 7. *If* $v \equiv 5 \pmod 8$, *then* $v \in P_4(4, 6)$.

Proof. $v = 4t + 1$, and by Lemma 1, $t + 1 \in P(\{4, 6\}, 1)$. Considering Proposition 8 it remains to be proved that $13 \in P_4(4, 6)$, $21 \in P_4(4, 6)$, $16 \in P_4''(4, 6)$, and $24 \in P_4''(4, 6)$. The first formula follows by Proposition 3 from (13).

Proof of

(18) $$21 \in P_4(4, 6).$$

Elements: (i, j) $(i = 0, 1, 2, 3;\ j = 0, 1, 2, 3, 4)$ and (A).
Blocks: Form all the quadruples on the sets

$$\{(A), (i, j): i = 0, 1, 2, 3\}, \qquad (j = 0, 1, 2, 3, 4).$$

and take them three times each. Further construct the system $P_4'[4, 6, 21]$ as follows:

$$\{(A), (a_0, j), (a_1, j - \alpha), (a_2, j + \alpha)\}, \qquad \left(\sum_{h=0}^{2} a_h \equiv 0 \pmod 2; \alpha = 1, 2\right);$$

$$\{(a_0, j), (a_1, j + 1), (a_2, j + 2), (a_3, j + 3)\} \qquad \left(\sum_{h=0}^{3} a_h \equiv 0 \pmod 4\right), \text{ twice;}$$

$$\{(a_0, j), (a_0 + 2, j), (a_1, j - \alpha), (a_2, j + \alpha)\} \qquad \Bigg(\alpha = 1, 2; \sum_{h=0}^{2} a_h \equiv \beta \pmod 4;$$

$$\text{for } \beta = 0 \text{ take the blocks once each and for } \beta = 1 \text{ twice each}\Bigg);$$

$\{(i, j), (i + 1, j), (i + \delta, j + \alpha), (i + \delta + 1, j + \alpha)\}$,
$(\alpha = 1, 2; \delta = 0, 1, 2, 3)$, three times.

The formula

(19) $$16 \in P_4''(4, 6)$$

follows directly from Propositions 3, 2, and 5; and

(20) $$24 \in P_4''(4, 6)$$

https://doi.org/10.4153/CJM-1963-069-5 Published online by Cambridge University Press

follows by Propositions 5 and 3 from $12 \in P_2''(4, 3)$ and this, considering (5), follows from (3).

LEMMA 8. *If* $v \equiv 1 \pmod 8$, *then* $v \in P(4, 6)$.

Proof. Let $v = 4t + 1$. By Lemma 1, $t + 2 \in P(\{4, 6\}, 1)$. By Proposition 9 it remains to be proved that $9 \in P(4, 6)$, $17 \in P(4, 6)$. Further, for suitably chosen classes T_2' and T_2'', $13 \in Q_4'(4, 6)$, $21 \in Q_4'(4, 6)$, $12 \in Q_4''(4, 6)$, $20 \in Q_4''(4, 6)$, and also $16 \in P_4''(4, 6)$ and $24 \in P_4''(4, 6)$. For the last two formulas see (19) and (20) respectively.

The relation

$$9 \in P(4, 6) \tag{21}$$

is obtained by taking all the quadruples on 9 elements.

Obviously $5 \in P(4, 2)$. Hence

$$17 \in P(4, 6) \tag{22}$$

follows by means of Propositions 4 and 3 from

$$17 \in P(5, 1), \tag{23}$$

which will now be proved.

Elements: (i) $\quad (i = 0, 1, \ldots, 16)$.

Blocks: $\{(i), (i + 1), (i + 2), (i + 8), (i + 11)\}$;
$\{(i), (i + 1), (i + 3), (i + 5), (i + 6)\}$;
$\{(i), (i + 1), (i + 4), (i + 9), (i + 14)\}$;
$\{(i), (i + 2), (i + 6), (i + 10), (i + 12)\}$.

In order to proceed we choose the class T_2' putting into it in addition to all those triples of T_2 which contain the element (A) also those triples which contain a pair of the form $\{(i, j), (i + 2, j)\}$. Thus T_2'' will contain those triples which contain a pair of the form $\{(i, j), (i + 1, j)\}$.

Proof of

$$13 \in Q_4'(4, 6). \tag{24}$$

Take three times the system $P_4'[4, 2, 13]$ used in (13) without the last set of blocks $\{(i, j), (i + 1, j), (i + \delta, j + 1), (i + \delta + 1, j + 1)\}$.

To prove

$$21 \in Q_4'(4, 6) \tag{25}$$

take the system $P_4'[4, 6, 21]$ used in (18) without the last set of blocks

$$\{(i, j), (i + 1, j), (i + \delta, j + \alpha), (i + \delta + 1, j + \alpha)\}.$$

Proof of

$$12 \in Q_4''(4, 6). \tag{26}$$

https://doi.org/10.4153/CJM-1963-069-5 Published online by Cambridge University Press

Elements: (i, j) $(i = 0, 1, 2, 3; j = 0, 1, 2)$.

Blocks: $\{(i, j), (i + 1, j), (i + \delta, j + 1), (i + \delta + 1, j + 1)\}$ $(\delta = 0, 1, 2, 3)$; $\{(i, j), (i + 1, j), (i + \delta, j - 1), (i + \eta, j + 1)\}$ $(\delta = 0, 1, 2, 3; \eta = 0, 1, 2, 3)$.

Proof of

$$20 \in Q_4''(4, 6). \tag{27}$$

Elements: (i, j) $(i = 0, 1, 2, 3; j = 0, 1, 2, 3, 4)$.

Blocks: $\{(a_0, j), (a_1, j + 1), (a_2, j + 2), (a_3, j + 3)\}$ $\left(\sum_{h=0}^{3} a_h \equiv 0 \pmod 4\right)$;

$\{(i, j), (i + 1, j), (i + \delta, j + \alpha), (i + \delta + 1, j + \alpha)\}$ $(\alpha = 1, 2; \delta = 0, 1, 2, 3)$, all the blocks taken three times.

LEMMA 9. *If* $v \equiv 1 \pmod{12}$, *then* $v \in P(4, 2)$.

Proof. Let $v = 6t + 1$. By Lemma 1, $t + 2 \in P(\{4, 6\}, 1)$. By Proposition 9 we have to prove that $13 \in P(4, 2)$, $25 \in P(4, 2)$, $24 \in P_6''(4, 2)$, $36 \in P_6''(4, 2)$ and, for suitably chosen T_2' and T_2'', $19 \in Q_6'(4, 2)$, $31 \in Q_6'(4, 2)$, $18 \in Q_6''(4, 2)$, and $30 \in Q_6''(4, 2)$. By Proposition 1 the first formula follows from (13).

Proof of

$$25 \in P(4,2). \tag{28}$$

Elements: (i, j) $(i = 0, 1, 2, 3, 4; j = 0, 1, 2, 3, 4)$.

Blocks: $\{(i, j), (i + 1, j), (i + 2, j), (i + 3, j)\}$;

$\{(a_0, j), (a_1, j + 1), (a_2, j + 2), (a_3, j + 3)\}$ $\left(\sum_{h=0}^{3} a_h \equiv 0 \pmod 5\right)$;

$\{(i, j), (i + \beta, j), (i + \eta, j + \alpha), (i + \eta + \beta, j + \alpha)\}$ $(\alpha = 1, 2; \beta = 1, 2; \eta = 0, 1, 2, 3, 4)$.

By Proposition 3,

$$24 \in P_6''(4, 2) \tag{29}$$

follows from

$$24 \in P_6''(4, 1) \tag{30}$$

which is a consequence of Propositions 2 and 5.

The formula

$$36 \in P_6''(4, 2) \tag{31}$$

follows from (8) by Propositions 3 and 5.

We now have to choose T_2' and T_2''. Every triple which appears in T_2 occurs there twice. If such a triple does not contain the element (A) we include it once in T_2' (in addition to all the triples which contain (A)) and once in T_2''.

https://doi.org/10.4153/CJM-1963-069-5 Published online by Cambridge University Press

Here, as well as in what follows, $m = 6$ (see Definition 5). We shall often denote the $m = 6$ elements by a pair of integers x, y ($x = 0, 1$; $y = 0, 1, 2$).

Proof of

$$19 \in Q_6'(4, 2). \tag{32}$$

Elements: (x, y, j) $\quad (x = 0, 1; y = 0, 1, 2; j = 0, 1, 2)$ and (A).

Blocks: $\{(A), (x_0, b_0, 0), (x_1, b_1, 1), (x_2, b_2, 2)\}$

$$\left(x_0, x_1, x_2 = 0, 1 \text{ independently}; \sum_{h=0}^{2} b_h \equiv 0 \pmod 3\right);$$

$\{(a_0, b_0, j), (a_0 + 1, b_0 + 1, j), (a_1, b_1, j + 1), (a_2, b_2, j + 2)\}$

$$\left(\sum_{h=0}^{2} a_h \equiv 0 \pmod 2; \sum_{h=0}^{2} b_h \equiv j \pmod 3\right);$$

$\{(x, y + 1, j), (x, y - 1, j), (x + \beta, y, j - 1), (x + \beta, y, j + 1)\}$ $\quad (\beta = 0, 1)$;
$\{(x, y, j), (x, y + 1, j), (x + 1, y, j - \epsilon), (x + 1, y + 1, j + \epsilon)\}$ $\quad (\epsilon = \pm 1)$;
$\{(x, y, j), (x, y + 1, j), (x, y, j + 1), (x, y + 1, j + 1)\}$;
$\{(0, y, j), (1, y, j), (0, y + \gamma, j + 1), (1, y + \gamma, j + 1)\}$ $\quad (\gamma = 0, 1, 2)$.

Proof of

$$31 \in Q_6'(4, 2). \tag{33}$$

Elements: (x, y, j) $\quad (x = 0, 1; y = 0, 1, 2; j = 0, 1, 2, 3, 4)$ and (A).

Blocks: $\{(A), (x + a_0, y + 1 + a_0, j), (x + a_1, y, j - \alpha), (x + a_2, y, j + \alpha)\}$

$$\left(a_h = 0, 1; \sum_{h=0}^{2} a_h \equiv 1 \pmod 2; \alpha = 1, 2\right);$$

$\{(a_0, y, j - \alpha), (a_1, y, j + \alpha), (a_2, y - \epsilon, j - 2\alpha), (a_3, y + \epsilon, j + 2\alpha)\}$

$$\left(\alpha = 1, 2; \epsilon = \pm 1; \sum_{h=0}^{3} a_h \equiv 0 \pmod 2\right);$$

$\{(a_0, y, j - 1), (a_1, y, j + 1), (a_2, y + \gamma, j - 2), (a_3, y + \gamma, j + 2)\}$

$$\left(\gamma = 0, 1, 2; \sum_{h=0}^{3} a_h \equiv 0 \pmod 2\right);$$

$\{(0, y + 1, j), (1, y + 1, j), (\beta, y - \eta, j - \alpha), (\beta + \eta, y - \eta, j + \alpha)\}$
$(\alpha = 1, 2; \beta = 0, 1; \eta = 0, 1)$;
$\{(x, y + 1, j), (x + \eta, y - 1, j), (\beta, y, j - \alpha), (\beta + \eta, y, j + \alpha)\}$
$(\alpha = 1, 2; \beta = 0, 1; \eta = 0, 1)$;
$\{(x, y, j), (x + \eta, y + 1, j), (\beta, y, j + \alpha), (\beta + \eta, y + 1, j + \alpha)\}$
$(\alpha = 1, 2; \beta = 0, 1; \eta = 0, 1)$;
$\{(0, y, j), (1, y, j), (0, y, j + \alpha), (1, y, j + \alpha)\}$ $\quad (\alpha = 1, 2)$.

Proof of

$$18 \in Q_6''(4, 2). \tag{34}$$

Elements: $(x, y, j) \qquad (x = 0, 1; y = 0, 1, 2; j = 0, 1, 2)$.
Blocks: $\{(a_0, b_0, j), (a_1, b_0 + 1, j), (a_2, b_1, j + 1), (a_3, b_2, j + 2)\}$

$$\left(\sum_{h=0}^{3} a_h \equiv 0 \pmod 2; \sum_{h=0}^{2} b_h \equiv j \pmod 3\right);$$

$\{(0, y, j), (1, y, j), (0, y + \gamma, j + 1), (1, y + \gamma, j + 1)\} \qquad (\gamma = 0, 1, 2)$.

Proof of

$$30 \in Q_6''(4, 2). \tag{35}$$

Elements: $(x, y, j) \qquad (x = 0, 1; y = 0, 1, 2; j = 0, 1, 2, 3, 4)$.
Blocks: $\{(a_0, b_0, j), (a_1, b_1, j + 1), (a_2, b_2, j + 2), (a_3, b_3, j + 3)\}$

$$\left(\sum_{h=0}^{3} a_h \equiv 0 \pmod 2; \sum_{h=0}^{3} b_h \equiv 0 \pmod 3\right);$$

$\{(x, y, j), (x, y + 1, j), (x + \beta, y, j + \alpha), (x + \beta, y + 1, j + \alpha)\}$
$(\alpha = 1, 2; \beta = 0, 1)$;
$\{(x, y + 1, j), (x, y - 1, j), (0, y, j + \epsilon\alpha), (1, y, j + \epsilon\alpha)\} \quad (\alpha = 1, 2; \epsilon = \pm 1)$;
$\{(0, y, j), (1, y, j), (0, y, j + \alpha), (1, y, j + \alpha)\} \qquad (\alpha = 1, 2)$;
$\{(x, y, j), (x + 1, y + 1, j), (x, y + \gamma, j + \alpha), (x + 1, y + \gamma + 1, j + \alpha)\}$
$(\alpha = 1, 2; \gamma = 0, 1, 2)$.

LEMMA 10. *If* $v \equiv 5 \pmod{12}$, *then* $v \in P(4, 2)$.

Proof. Put $v = 6t + 5$. By Lemma 1, $t + 2 \in P(\{4, 6\}, 1)$. Considering Proposition 9 we have to prove

(a) the existence of systems $P[4, 2, 17]$ and $P[4, 2, 29]$ such that each of them includes a system $P[4, 2, 5]$,

(b) $24 \in P_6''(4, 2)$ and $36 \in P_6''(4, 2)$,

(c) if T_2' and T_2'' are chosen in the same way as in the proof of Lemma 9, then $23 \in Q_6'(4, 2)$, $35 \in Q_6'(4, 2)$ and

(d) $18 \in Q_6''(4, 2)$ and $30 \in Q_6''(4, 2)$.

For (b) see (29) and (31), and for (d), (34) and (35) respectively. As for (a), the existence of the required system $P[4, 2, 17]$ follows from (23), and that of $P[4, 2, 29]$ follows from Lemma 7 with some changes in its proof. Clearly $29 \equiv 5 \pmod 8$ and $29 = 4 \times 7 + 1$. In this case $t + 1 = 8 \in P(4, 1)$ by Lemma 4, and in order to prove $29 \in P(4, 2)$ it remains to show that $13 \in P_4(4, 2)$—for which see (13)—and that $16 \in P_4''(4, 2)$ which follows from Propositions 3, 2, and 5. It remains to prove (c).

Proof of

$$23 \in Q_6'(4, 2). \tag{36}$$

Elements: $(x, y, j) \qquad (x = 0, 1; y = 0, 1, 2; j = 0, 1, 2)$ and (A, s)
$(s = 0, 1, 2, 3, 4)$.

https://doi.org/10.4153/CJM-1963-069-5 Published online by Cambridge University Press

Blocks: $\{(A, \gamma), (a_0, b_0, 0), (a_1, b_1, 1), (a_2, b_2, 2)\}$

$$\left(\sum_{h=0}^{2} a_h \equiv 1 \pmod 2; \sum_{h=0}^{2} b_h \equiv \gamma \pmod 3; \gamma = 0, 1, 2\right) \text{ twice;}$$

$\{(A, \beta + 3), (a_0, b_0, 0), (a_1, b_1, 1), (a_2, b_2, 2)\}$

$$\left(\sum_{h=0}^{2} a_h \equiv 0 (\mathrm{mod}\ 2); \sum_{h=0}^{2} b_h \equiv \epsilon\beta (\mathrm{mod}\ 3), \epsilon = \pm 1; \beta = 0, 1\right);$$

$\{(a_0, y + 1, j), (a_0, y - 1, j), (a_1, y, j - 1), (a_2, y, j + 1)\}$

$$\left(\sum_{h=0}^{2} a_h \equiv 0 (\mathrm{mod}\ 2)\right);$$

$\{(x, y, j), (x, y + 1, j), (x + \beta, y, j + 1), (x + \beta, y + 1, j + 1)\}$ $(\beta = 0, 1)$;
$\{(0, y, j), (1, y + \gamma, j), (0, y + \delta, j + 1), (1, y + \gamma + \delta, j + 1)\}$
$(\gamma = 0, 1, 2; \delta = 0, 1, 2)$.

Proof of

$$35 \in Q_6'(4, 2). \tag{37}$$

Elements: (x, y, j) $(x = 0, 1; y = 0, 1, 2; j = 0, 1, 2, 3, 4)$ and (A, s)
$(s = 0, 1, 2, 3, 4)$.

Blocks: $\{(A, 2\beta + \eta), (x + \beta + \delta, y, j), (x, y + \delta(1 + \eta), j - \alpha),$
$(x, y + (1 - \delta)(1 + \eta), j + \alpha)\}$ $(\alpha = 1, 2; \beta = 0, 1; \delta = 0, 1; \eta = 0, 1)$;
$\{(A, 2\beta + \eta), (x + \beta, y, j), (x + 1, y - \delta(1 + \eta), j - \alpha),$
$(x, y - (1 - \delta)(1 + \eta), j + \alpha)\}$ $(\alpha = 1, 2; \beta = 0, 1; \delta = 0, 1; \eta = 0, 1)$;
$\{(A, 4), (x + a_0, y + 1 + a_0, j), (x + a_1, y, j - \alpha), (x + a_2, y, j + \alpha)\}$

$$\left(a_h = 0, 1; \sum_{h=0}^{2} a_h \equiv 1 (\mathrm{mod}\ 2); \alpha = 1, 2\right);$$

$\{(a_0, y, j - \alpha), (a_1, y, j + \alpha), (a_2, y - \epsilon, j - 2\alpha), (a_3, y + \epsilon, j + 2\alpha)\}$

$$\left(\alpha = 1, 2; \epsilon = \pm 1; \sum_{h=0}^{3} a_h \equiv 0 (\mathrm{mod}\ 2)\right);$$

$\{(a_0, y, j), (a_1, y, j + 1), (a_2, y, j + 2), (a_3, y, j + 3)\}$

$$\left(\sum_{h=0}^{3} a_h \equiv 0 (\mathrm{mod}\ 2)\right);$$

$\{(0, y + 1, j), (1, y + 1, j), (\beta, y - \eta, j - \alpha), (\beta + \eta, y - \eta, j + \alpha)\}$
$(\alpha = 1, 2; \beta = 0, 1; \eta = 0, 1)$;
$\{(x, y + 1, j), (x + \eta, y - 1, j), (\beta, y, j - \alpha), (\beta + \eta, y, j + \alpha)\}$
$(\alpha = 1, 2; \beta = 0, 1; \eta = 0, 1)$;
$\{(x, y, j), (x + \eta, y + 1, j), (\beta, y, j + \alpha), (\beta + \eta, y + 1, j + \alpha)\}$
$(\alpha = 1, 2; \beta = 0, 1; \eta = 0, 1)$;
$\{(0, y, j), (1, y, j), (0, y, j + \alpha), (1, y, j + \alpha)\}$ $(\alpha = 1, 2)$.

https://doi.org/10.4153/CJM-1963-069-5 Published online by Cambridge University Press

LEMMA 11. *If* $v \equiv 2 \pmod{12}$, *then* $v \in P(4, 1)$.

Proof. For $v \equiv 26 \pmod{36}$ see the proof in **(6**, Section 3.4**)**. For $v \equiv 2$ or $14 \pmod{36}$, $v = 6t + 2$ and by Lemmas 3 and 4 and an assumption of induction we may assume that $t + 2 \in P(4, 1)$. By Proposition 9, we have to prove that $14 \in P(4, 1)$; further that, for suitably chosen T_2' and T_2'', $20 \in Q_6'(4, 1)$ and $18 \in Q_6''(4, 1)$ and that $24 \in P_6''(4, 1)$. For the last formula see (30). We prove

(38) $$14 \in P(4, 1).$$

Elements: (i, j) $\quad (i = 0, 1; j = 0, 1, \ldots, 6)$.

Blocks: $\{(i, j), (i, j - (-1)^i 2^0), (i, j - (-1)^i 2^1), (i, j - (-1)^i 2^2)\}$;
$\{(i + 1, j), (i, j + (-1)^i 2^0), (i, j + (-1)^i 2^1), (i, j + (-1)^i 2^2)\}$;
$\{(0, j), (1, j), (0, j + 2^\gamma), (1, j + 2^\gamma)\}$ $\quad (\gamma = 0, 1, 2)$;
$\{(0, j), (0, j + 2^\gamma), (1, j + 3^{1+3\beta+2\gamma}), (1, j + 3^{2+3\beta+2\gamma})\}$ $\quad (\beta = 0, 1; \gamma = 0, 1, 2)$.

We choose the classes T_2' and T_2'' in a way similar to that described in the proof of Lemma 8. We include in T_2'' all those triples of T_2 which contain a pair of the form $\{(i, j), (i + 1, j)\}$. All the other triples of T_2 are included in T_2'.

Proof of

(39) $$20 \in Q_6'(4, 1).$$

Elements: (i, j) $\quad (i = 0, 1, \ldots, 5; j = 0, 1, 2)$ and (A, s) $\quad (s = 0, 1)$.

Blocks: $\{(A, s), (a_0, 0), (a_1, 1), (a_2, 2)\}$ $\quad \left(\sum_{h=0}^{2} a_h \equiv 3s \pmod 6\right)$;

$\{(i, j), (i + 2, j), (i + 3\beta + 1, j - 1), (i + 3\beta + 1, j + 1)\}$ $\quad (\beta = 0, 1)$;
$\{(i, j), (i + 2, j), (i + 3, j - \epsilon), (i + 5, j + \epsilon)\}$ $\quad (\epsilon = \pm 1)$;
$\{(i, j), (i + 2, j), (i, j + 1), (i + 2, j + 1)\}$;
$\{(\gamma, j), (\gamma + 3, j), (\delta, j + 1), (\delta + 3, j + 1)\}$ $\quad (\gamma = 0, 1, 2; \delta = 0, 1, 2)$.

Proof of

(40) $$18 \in Q_6''(4, 1).$$

Elements: (i, j) $\quad (i = 0, 1, \ldots, 5; j = 0, 1, 2)$.

Blocks: $\{(a_0, j), (a_0 + 1, j), (a_1, j + 1), (a_2, j + 2)\}$

$$\left(\sum_{h=0}^{2} a_h \equiv 2j \pmod 6\right).$$

4. Finite Möbius planes. Let p be a power of a prime, and let G be a Galois field of order p **(**see **3**, pp. 242–288**)**. Further let F be a Galois field of order p^2 constructed over G, the elements of which are the roots of an irreducible equation in G

(41) $$t^2 = A + A't \qquad (A, A' \in G).$$

https://doi.org/10.4153/CJM-1963-069-5 Published online by Cambridge University Press

In what follows the elements of G will be denoted by small italics (with the exception of A, A' in (41)) and those of F by Greek letters, $\alpha = a + a't$. The zero element of F will be $\phi = 0 + 0 . t$.

We extend the field F to F^* by adding an element ∞ which has no representation in the form $a + a't$ and for which we define the field operations as follows:

$$\begin{aligned} \xi + \infty &= \infty && \text{for } \xi \neq \infty, \\ \xi . \infty &= \infty && \text{for } \xi \neq \phi, \\ \xi / \infty &= \phi && \text{for } \xi \neq \infty, \\ \xi / \phi &= \infty && \text{for } \xi \neq \phi; \end{aligned}$$

the expressions $\infty + \infty$, $\phi . \infty$, ∞ / ∞, and ϕ / ϕ have no meaning.

If the element ∞ will be adjoint to the field G, we shall denote $G^* = G \cup \{\infty\}$.

DEFINITION 6. *A transformation*

$$\eta = T(\xi) = \frac{\alpha\xi + \beta}{\gamma\xi + \delta} \qquad (\alpha, \beta, \gamma, \delta \neq \infty, \alpha\delta - \beta\gamma \neq \phi) \tag{42}$$

is called a linear transformation.

In a similar way as in fields of characteristic 0 (see **1**, pp. 22–28) the following propositions can be easily proved.

PROPOSITION 10. *A linear transformation is one–one.*

PROPOSITION 11. *The linear transformations form a group.*

DEFINITION 7. *The cross ratio*

$$(\xi_1, \xi_2, \xi_3, \xi_4) = \frac{\xi_1 - \xi_2}{\xi_1 - \xi_4} \Big/ \frac{\xi_3 - \xi_2}{\xi_3 - \xi_4} \tag{43}$$

is the image of ξ_1 under the linear transformation which carries ξ_2, ξ_3, ξ_4 into ϕ, $1, \infty$ respectively.

The following definition has been suggested by Professor E. Jabotinsky.

DEFINITION 8. *A subset S of F^* is a circle if*

$$(\xi_1, \xi_2, \xi_3, \xi_4) \in G \tag{44}$$

for any four mutually distinct elements $\xi_1, \xi_2, \xi_3, \xi_4$ of S and if no set properly containing S has this property.

DEFINITION 9. *If S is a circle and if there are three mutually distinct elements ξ_1, ξ_2, ξ_3 of S such that*

$$\frac{\xi_1 - \xi_2}{\xi_1 - \xi_3} \in G,$$

then S will be called a line. A circle which is not a line is a proper circle.

Again as in **(1)** it can be proved that

PROPOSITION 12. *A linear transformation transforms circles into circles.*

Evidently the set $\{a + 0 . t, \infty : a \in G\}$ isomorph to G^* is a circle and even a line. Propositions 10 and 12 imply the following propositions.

PROPOSITION 13. *For any two circles there exists a linear transformation transforming one of them into the other.*

PROPOSITION 14. *For any three elements of F^*, there exists exactly one circle containing them.*

PROPOSITION 15. *Every circle has $p + 1$ elements.*

DEFINITION 10. *The extended field F^* with the system of circles on it forms a finite Möbius plane of rank p, $MG\ (p, 2)$.*

PROPOSITION 16. *The system of lines in a finite Möbius plane of rank p forms, after deleting the element ∞, a finite Euclidean plane of rank p, $EG(p, 2)$*; (see **3**, pp. 323–354).

From Propositions 14 and 15 we have the following theorem.

THEOREM 2. *If p is a power of a prime, then there exists a configuration $C[p + 1, 3, 1, p^2 + 1]$. Especially $MG(p, 2)$ is such a configuration.*

LEMMA 12. *Let $v \geqslant 35$. Then $v \in P(K_v, 1)$, where*

$$K_v \equiv \{n : 4 \leqslant n < 5/4\sqrt{v} + 1\}.$$

Proof. For $x \geqslant 24$ there is always a prime between x and $5x/4$. By checking the smaller values of x it is easily established that for $x \geqslant 8$ there exists always a prime power q such that

$$4x/5 < q < x. \tag{45}$$

Let p be the smallest prime power satisfying $p > \sqrt{v}$. Then $p < 5/4\sqrt{v}$. We shall prove that

$$v \in P(\{n : 4 \leqslant n \leqslant p + 1\}, 1) \qquad \text{for } v \geqslant 35 \tag{46}$$

Consider the $MG(p, 2)$, delete the element ∞, and choose a family D of p parallel (i.e. disjoint) lines. Delete all or some elements on $d = [\frac{1}{2}(p - 3)]$ of these lines in such a way that on none of these lines exactly three elements remain. As long as $d \geqslant 2$ any number w, $0 \leqslant w \leqslant dp$, of elements may be thus deleted. What remains is evidently a system $P[\{n : 4 \leqslant n \leqslant p + 1\}, 1, p^2 - w]$.

Clearly w can obtain all the values

$$0 \leqslant w \leqslant \tfrac{1}{2}p(p - 4) \tag{47}$$

and if p is odd, even the values

$$(48) \qquad 0 \leqslant w \leqslant \tfrac{1}{2}p(p-3).$$

If $p \geqslant 16$ there exists by (45) a prime power $p' < p$ and a value w satisfying (47) such that $p^2 - w = (p')^2$. For $8 \leqslant p < 16$ the existence of such a p' for which there exists a value w satisfying (47) or (48), and such that $p^2 - w = (p')^2$ can be checked directly. For $p = 7$, $0 \leqslant w \leqslant 14$. Thus (46) is proved.

From Lemma 12 and Propositions 4 and 2 follows:

COROLLARY 1. $v \in P(\{n : 4 \leqslant n \leqslant 34\}, 1)$ *holds for every* $v \geqslant 4$.

LEMMA 13. *Let* $v \geqslant 4$. *Then* $v \in P(4, 12)$.

Proof. By Proposition 4 and Corollary 1, it is sufficient to show that our lemma is true if $4 \leqslant v \leqslant 34$. By Proposition 3 this follows from Lemmas 2–11 for all these values of v, except 15 and 27. We now prove that

$$(49) \qquad 15 \in P(4, 12).$$

The configuration $P[4, 12, 15]$ is obtained by taking all the quadruples out of 15 elements.

Proof of

$$(50) \qquad 27 \in P(4, 12).$$

Elements: (g) where $g = a_0 + a_1 t + a_2 t^2$ $(a_i = 0, 1, 2;\ i = 0, 1, 2)$ are elements of a Galois field G_{27} of order 27, with $x^3 = x + 2$.

Blocks: $\{(g), (g + x^{\alpha}), (g + x^{\alpha+5}), (g + x^{\alpha+10})\}$ $(\alpha = 0, 1, \ldots, 25)$;
$\{(g), (g + x^{\alpha}), (g + x^{\alpha+1}), (g + x^{\alpha+13})\}$ $(\alpha = 0, 1, \ldots, 25)$, twice;
$\{(g), (g + x^{2\beta}), (g + x^{2\beta+1}), (g + x^{2\beta+16})\}$ $(\beta = 0, 1, \ldots, 12)$, 9 times;
$\{(g), (g + x^{2\beta}), (g + x^{2\beta+8}), (g + x^{2\beta+12})\}$ $(\beta = 0, 1, \ldots, 12)$, 9 times;
$\{(g), (g + x^{2\beta}), (g + x^{2\beta+3}), (g + x^{2\beta+22})\}$ $(\beta = 0, 1, \ldots, 12)$.

If $\alpha = a + a't$ and $\beta = b + b't$ are elements of a finite Möbius plane of an odd rank, we may adopt the usual terminology:

$$(51) \qquad \bar{\alpha} = a + A'a' - a't$$

is the element *conjugate* to α;

$$(52) \quad (\alpha, \beta) = \tfrac{1}{2}(\alpha\bar{\beta} + \bar{\alpha}\beta) = ab - Aa'b' + \tfrac{1}{2}A'(ab' + a'b), \ (\alpha, \infty) = 0,$$

is the *scalar product* of α and β;

$$(53) \qquad |\alpha| = (\alpha, \alpha) = \alpha\bar{\alpha} = a^2 - Aa'^2 + A'aa'$$

is the *absolute value* of α;

$$(54) \qquad |\beta - \alpha|$$

is the *distance* between α and β.

This enables us to give a more geometrical definition of a circle in fields of odd rank. In particular the following theorem can easily be proved.

THEOREM 3. *A necessary and sufficient condition for $S \subset F^*$ to be a proper circle is the existence of elements $\mu \in F$ and $r \in G$ $(\mu, r \neq \infty)$ such that*

$$|\xi - \mu| = r \tag{55}$$

if and only if $\xi \in S$.

A necessary and sufficient condition for $S \subset F^*$ to be a line is the existence of elements $\varphi, \psi \in F$ $(\varphi \neq \phi)$ such that

$$(\varphi, \xi - \psi) = 0 \tag{56}$$

if and only if $\xi \in S$.

REFERENCES

1. L. V. Ahlfors, *Complex analysis* (New York, 1953).
2. R. C. Bose, *On the construction of balanced incomplete block designs*, Ann. Eugenics, *9* (1939), 353–399.
3. R. D. Carmichael, *Groups of finite order* (New York, 1956).
4. M. Hall, Jr. and W. S. Connor, *An embedding theorem for balanced incomplete block designs*, Can. J. Math., *6* (1954), 35–41.
5. H. Hanani, *On quadruple systems*, Can. J. Math., *12* (1960), 145–157.
6. ——— *The existence and construction of balanced incomplete block designs*, Ann. Math. Stat., *32* (1961), 361–386.
7. E. H. Moore, *Concerning triple systems*, Math. Ann., *43* (1893), 271–285.
8. H. K. Nandi, *On the relation between certain types of tactical configurations*, Bull. Calcutta Math. Soc., *37* (1945), 92–94.
9. M. Reiss, *Ueber eine Steinersche combinatorische Aufgabe*, J. reine angew. Math., *56* (1859), 326–344.
10. S. S. Shrikhande, *The impossibility of certain symmetrical balanced incomplete block designs*, Ann. Math. Stat., *21* (1950), 106–111.
11. G. Tarry, *Le problème des 36 officiers*, Compt. rend. assoc. franc. av. sci. *1* (1900), 122–123 and *2* (1901), 170–203.

Technion, Israel Institute of Technology,
Haifa, Israel