PROCEEDINGS OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 91, Number 3, July 1984

CONSTRUCTING PRIME-FIELD PLANAR CONFIGURATIONS

GARY GORDON

ABSTRACT. An infinite class of planar configurations is constructed with distinct prime-field characteristic sets (i.e., configurations represented over a finite set of prime fields but over fields of no other characteristic). It is shown that if p is sufficiently large, then every subset of k primes between p and $f(p, k)$ forms such a set (where $f(p, k) = 2^{[(\sqrt{p} - Ak^{3/2})/Bk^{3/2}]}$ for constants A and B). In particular, for every positive integer k, there exist infinitely many planar matroid configurations $C_{i,k}$ with $|\chi_{pf}(C_{i,k})| = k$ (where $\chi_{pf}(C)$ denotes the prime-field characteristic set of C). We also give a result concerning cofinite prime-field characteristic sets.

1. Introduction. We are interested in the problem of constructing finite configurations C of points and lines such that C can be represented precisely over fields of given characteristics, where the characteristics have been previously specified. More precisely, for a planar configuration C of points and lines, define the *characteristic set* $\chi(C)$ to be a set of primes (perhaps including zero) such that $p \in \chi(C)$ if and only if there is some field F of characteristic p and some subset C' of the projective plane $PG(2, F)$ such that C and C' have the same incidences. Let $P = \{0, 2, 3, 5, \dots\}$ denote the set of all field characteristics. Then $\chi \subseteq P$ is a *characteristic set* if $\chi = \chi(C)$ for some configuration C. Finally, if there is a C such that $p \in \chi(C)$ implies C can be embedded in $PG(2, p)$, we call χ a *prime-field characteristic set*, and denote it $\chi_{pf}(C)$ or χ_{pf}.

Since such finite configurations are planar matroids, we can restate the above definitions in terms of matroid representation theory. In these terms, $p \in \chi(C)$ if there is a field F of characteristic p and a rank three matrix M with entries in F such that:

(1) There is a one-to-one correspondence between the points of C and the columns of M.

(2) Three points are collinear in C if and only if the corresponding three columns of M are linearly dependent.

In what follows, we use the terms "matroid", "configuration" and "matroid configuration" interchangeably to refer to a rank three matroid. In addition, we use "point" (of C) and "column" (of M) interchangeably, when no confusion can arise.

Characteristic sets for matroids were formally defined by Ingleton [**6**], while prime-field sets were introduced by Brylawski [**1**]. The study of possible characteristic sets, however, appears implicitly in the work of Pappus, Pascal, Descargues and

Received by the editors September 23, 1982 and, in revised form, September 27, 1983.
1980 *Mathematics Subject Classification*. Primary 05B35, 51E20, 51D20.
Key words and phrases. Matroid configuration, characteristic set, prime-field characteristic set.

Fano. Subsequently, it has been shown that:

(1) $0 \in \chi(C) \Rightarrow \chi(C)$ is cofinite (Rado [8]).

(2) $\chi(C)$ infinite $\Rightarrow 0 \in \chi(C)$ (Vamos [11]).

(3) Every cofinite characteristic set (necessarily including 0) is realizable (Reid unpublished but see [2]).

(4) All finite characteristic sets (necessarily excluding 0) are realizable (Kahn [7]).

The questions concerning both finite and cofinite characteristic sets were solved using fields which contain many transcendentals. Thus the corresponding questions about prime-field sets remain open.

It is well known that $\chi_{pf}(PG(2, p)) = \{p\}$, and so all singletons in P (except $\{0\}$) form prime-field sets. Reid [9] exhibited the first two element prime-field set when he constructed a configuration C with $\chi_{pf}(C) = \{1103, 2089\}$. Brylawski and Reid [2] generalized these techniques to construct many finite, nonsingleton prime-field sets. (Reid's example was the first two element characteristic set, as well.)

The main result of this paper, Theorem 4.1, says that for every $k > 0$, every subset of primes $p_1 < p_2 < \cdots < p_k$ with p_1 sufficiently large and

$$p_k < 2^{[(\sqrt{p_1} - Ak^{3/2})/Bk^{3/2}]}$$

for fixed constants A and B, independent of k and $p_1, \ldots, p_k$, forms a prime-field characteristic set. Thus, for all $k > 0$, there are infinitely many prime-field sets containing exactly k primes.

§§2–4 below are concerned with constructing finite prime-field characteristic sets.

Finally, we thank Professor Tom Brylawski for his helpful conversations and Professor William Lenhart for computing assistance.

2. Background construction. Our goal in §§2–4 is to construct finite prime-field characteristic sets. To determine χ or χ_{pf} for a given configuration C, it is useful to construct a representing matrix (when $\chi \neq \varnothing$) in a canonical way.

DEFINITION 2.1. Two matrices A_1 and A_2 over F are *projectively equivalent* if one can be obtained from the other by a sequence of the following operations:

(1) elementary row operations,

(2) multiplication of columns by nonzero scalars,

(3) an automorphism of F,

(4) removal of a row of zeros.

Since each of these operations preserves column dependences, projectively equivalent matrices represent isomorphic matroid configurations. A matroid C (with $\chi(C) \neq \varnothing$) is *projectively unique* if any two matrices which represent it (over F) are projectively equivalent. Finally, a matroid C is *sequentially unique* if there is an ordering of the points of $C = \{x_1, \ldots, x_n\}$ such that for each $1 \leqslant i \leqslant n$, the submatroid $\{x_1, \ldots, x_i\}$ is projectively unique.

For planar configurations (rank 3 matroids), this means that we can assume the first four points of C form a quadrangle (a matroid circuit), and each successive point is on at least two lines generated by previous points. For such configurations, determining χ amounts to examining all subdeterminants of the representing matrix.

Given k primes $p_1 < p_2 < \cdots < p_k$ with $k \geqslant 2$, we will construct a configuration which satisfies two conditions.

I. All but the primes $p_1, \ldots, p_k$ are eliminated from χ_{pf}.

II. No prime $p_1, \ldots, p_k$ itself was eliminated in the process.

To satisfy condition I, we will construct a configuration C such that any matrix representing C (over the prime p_1) will contain a subdeterminant equal to a nonzero multiple of $p_1 \cdots p_k$. This is accomplished by using the von Staudt calculus and results of **[3]** to do arithmetic synthetically. We then introduce a dependence which forces this product to be zero. This will eliminate all characteristics not dividing $p_1 \cdots p_k$, and thus satisfy I. Condition II, however, requires more careful work.

Although much of what follows is quite algebraic, the reader should keep in mind the underlying geometric structure. We are only concerned with representing point-line incidences with the column dependences of a matrix.

Let $p_1 < p_2 < \cdots < p_k$ be our finite set of primes and set $N = p_1 \cdot p_2 \cdots p_k + 2$. Let b_i denote the integer represented by the first i digits of the binary expansion of N. Thus, $b_1 = 1$, $b_2 = 2$ or 3, and, in general, $b_{i+1} = 2b_i$ or $2b_i + 1$. This is the general binary construction in **[1]**.

In **[1]**, this b_i sequence is used in constructing a sequentially unique planar configuration C satisfying I above (i.e., $\chi_{pf}(C) \subseteq \{ p_1, \ldots, p_k \}$). Among other features, this configuration has one line containing distinct points corresponding to each b_i ($1 \leqslant i \leqslant \log_2 N + 1$). Thus, for example, if $p_1 = 5$ and $p_2 = 7$ (with $k = 2$), then $N = 37$ and this line contains six points corresponding to the six b_i values $1, 2, 4, 9, 18, 37$. But $b_3 = 4 \equiv 9 = b_4 \pmod 5$, and so these two points form a multiple point (a two-point circuit) over the prime 5, a dependence not replicated over 7. Thus II above is not satisfied in this example.

We circumvent this problem in two ways. First, we modify the b_i sequence to avoid certain "bad" values, e.g., $b_i \equiv 0 \pmod{p_1}$ but $b_i \not\equiv 0 \pmod{p_2}$. Second, we use projective cross ratios to preserve the b_i coordinate values from one line to another, so the resulting configuration will not contain a "bad" line, as above. This avoids the problem $b_i \equiv b_j \pmod{p_1}$ but $b_i \not\equiv b_j \pmod{p_2}$.

In Figure 2.2 below, each line l_i will contain points with coordinates involving a modification of our b_i sequence. These lines all meet at the point 0. The points P_i are used to project certain points from l_i to l_{i+1} by preserving specified cross ratios.

We now modify the b_i sequence. Let $\bar{b}_i = b_i$ for $i = 1, 2$ and 3. In general, we define $\bar{b}_i$ inductively. Consider the following matrix $M(i)$:

$$\begin{bmatrix} 1 & 0 & 0 & 1 & 1 & 0 & 1 & 1 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 1 & 1 & 1 & -r_{i-1} & 0 & 1 & 2 & 1 & 1 \\ 0 & 0 & 1 & 1 & 0 & 1 & 0 & r_{i-1} & \bar{b}_{i-1} & \bar{b}_i & \bar{b}_i & \bar{b}_{i-2} \end{bmatrix},$$

where $\bar{b}_i = 2\bar{b}_{i-1} + r_{i-1}$ and $i \geqslant 4$. ($M(i)$ will be a fundamental building block in our construction. For now, we use its 3×3 subdeterminants to determine which possible values for $\bar{b}_i$ are to be avoided.)

Now consider all 3×3 subdeterminants of $M(i)$ involving the term $\bar{b}_i$. There are at most $\binom{12}{3} = 220$ such subdeterminants, and many of these will not involve $\bar{b}_i$. In any case, let D be the constant denoting the number of subdeterminants involving $\bar{b}_i$ in a nontrivial way.

We assume inductively that $\bar{b}_1, \bar{b}_2, \ldots, \bar{b}_{j-1}$ have all been defined so that:

(∗) None of the D subdeterminants of $M(i)$ vanish (mod p_m) for any m.

We also assume, for $i < j$,

A. $|\bar{b}_i - b_i| \leqslant D \cdot k$,

B. $\bar{b}_i = 2\bar{b}_{i-1} + r_{i-1}$, where $|r_{i-1}| \leqslant 3D \cdot k + 1$.

Now define $\bar{b}_j$ to be the integer closest to b_j so that (∗) holds for $M(j)$. (If this choice is not unique, we arbitrarily select the larger value.)

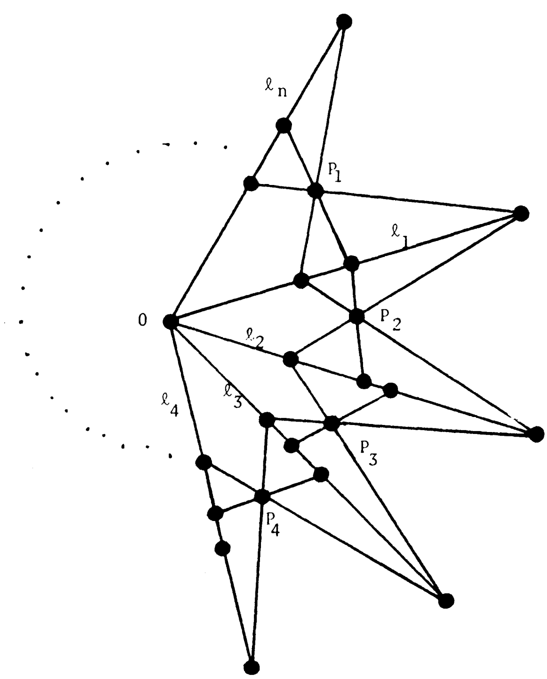

FIGURE 2.2

LEMMA 2.3. *Suppose $6D \cdot k < p_1 < \cdots < p_k$. Then the integer $\bar{b}_j$ defined above satisfies* A *and* B.

PROOF. For condition A, we note that each of the D subdeterminants of $M(j)$ involving $\bar{b}_j$ is at most a quadratic expression in $\bar{b}_j$ (since the first row of $M(j)$ contains no $\bar{b}_j$ or r_{j-1} terms). Thus any subdeterminant S involving $\bar{b}_j$ nontrivially can be congruent to zero (mod p_m) for some m for at most $2k$ distinct integers near b_j (i.e., in the interval $[b_j - D \cdot k, b_j + D \cdot k]$). Thus, at most $2k \cdot D$ potential choices for $\bar{b}_j$ have been ruled out. Since $\bar{b}_j$ is the integer closes to b_j avoiding these (at most) $2k \cdot D$ choices, we must have $|\bar{b}_j - b_j| < D \cdot k$ and A is satisfied. For B, we have

$$\begin{aligned}|\bar{b}_j - 2\bar{b}_{j-1}| &\leqslant |\bar{b}_j - b_j| + |b_j - 2b_{j-1}| + 2|b_{j-1} - \bar{b}_{j-1}| \\ &\leqslant D \cdot k + 1 + 2D \cdot k = 3D \cdot k + 1.\end{aligned}$$

This completes the proof.

3. Construction of the matrix $M(N)$. As before, assume $6D \cdot k < p_1 < \cdots < p_k$ and set $N = p_1 \cdots p_k + 2$. Define the $\bar{b}_i$ sequence as in the previous section. We will not construct a matrix whose column dependences over p_1 give a configuration with characteristic set $\{p_1, \ldots, p_k\}$.

In Part 1 below, we construct a matrix whose coordinates contain all the possible values r_i can assume (where $\bar{b}_{i+1} = 2\bar{b}_i + r_i$, $|r_i| \leqslant 3D \cdot k + 1$). Appropriate r_i values will then be preserved by projecting corresponding points onto lines created in Part 2.

PART 1. *r_i submatrix.* Let $t = 3D \cdot k + 1$ and let M_1 be

$$\begin{array}{ccccccccccccccccccc} a_1 & a_2 & a_3 & a_4 & a_5 & a_6 & a_7 & a_8 & a_9 & a_{10} & a_{11} & a_{12} & \cdots & & & & & & a_{3t+6} \\ 1 & 0 & 0 & 1 & 1 & 1 & 0 & 1 & 2 & 1 & 1 & 1 & 1 & 1 & 1 & & 1 & 1 & 1 \\ 0 & 1 & 0 & 1 & 1 & 0 & 1 & -1 & 0 & 2 & 2 & -2 & 3 & 3 & -3 & \cdots & t & t & -t \\ 0 & 0 & 1 & 1 & 0 & 1 & 1 & 0 & 1 & 1 & 0 & 0 & 1 & 0 & 0 & & 1 & 0 & 0 \end{array}$$

If we take column dependences of M_1 over p_1, thus creating a matroid configuration C_1, we get the following proposition.

PROPOSITION 3.1. *C_1 is sequentially unique.*

PROOF. Results of [3] allow us to assume columns a_1–a_4 are uniquely determined. For $i \geqslant 4$ we list the two dependences which determine each column a_i uniquely over the integers (and hence over the prime subfield of any field).

$$\begin{array}{lll} a_5\colon a_1a_2,\, a_3a_4 & a_{10}\colon a_2a_4,\, a_5a_7 & \\ a_6\colon a_1a_3,\, a_2a_4 & a_{3i-1}\colon a_1a_2,\, a_3a_{3i-2} & \text{for } 4 \leqslant i \leqslant t+2, \\ a_7\colon a_1a_4,\, a_2a_3 & & \\ a_8\colon a_1a_2,\, a_6a_7 & a_{3i}\colon a_1a_2,\, a_9a_{3i-2} & \text{for } 4 \leqslant i \leqslant t+2, \\ a_9\colon a_1a_3,\, a_4a_8 & a_{3i+1}\colon a_2a_4,\, a_7a_{3i-1} & \text{for } 4 \leqslant i \leqslant t+1. \end{array}$$

PART 2. *$\bar{b}_i$ submatrices.* We wish to construct a matrix whose coordinates contain our $\bar{b}_i$ sequence. Consider the matrix $M_2(i)$ for $1 \leqslant i \leqslant n$ (where $\bar{b}_{n+1} = b_{n+1} = N$):

$$\begin{array}{c} \begin{array}{cccccccccccc} A & B & C & D & E & F & G & H & I & J & K & L \end{array} \\ \begin{bmatrix} 1 & 0 & 0 & 1 & 1 & 0 & 1 & 1 & 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 & 1 & 1 & -r_i & 0 & 2 & 1 & 2 & 1 \\ 0 & 0 & 1 & 1 & 0 & 1 & 0 & r_i & 1 & \bar{b}_i & \bar{b}_{i+1} & \bar{b}_{i+1} \end{bmatrix} \end{array}$$

(Compare with matrix $M(i)$ in §2.) Note that $M_2(1)$ (with columns G and J deleted) gives a sequentially unique matroid (over p_1 or over the integers). In general, $M_2(i)$ will have all its coordinates uniquely determined once columns G and J have been determined.

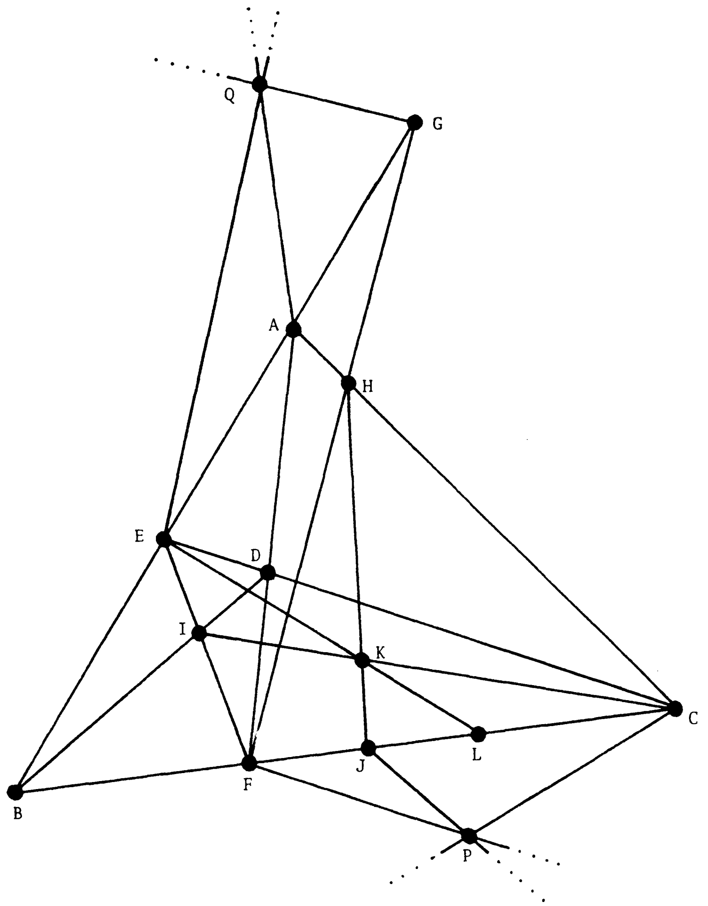

FIGURE 3.2

Our basic idea is to "recode" $M_2(i)$ by introducing a transcendental x_i in the coordinates for A, B, and D. Column G will be determined by projecting the appropriate r_i value from the line $z = 0$ in M_1, while column J will be determined (for $i > 1$) by projecting the point corresponding to column L in $M_2(i-1)$. The configuration resulting from this is pictured in Figure 3.2.

More precisely, let $x_1, \ldots, x_n$ be independent transcendentals, where $\bar{b}_{n+1} = N$ is the last term in the $\bar{b}_i$ sequence. For $1 \leqslant j \leqslant n$, we define the "recoded" matrix $M(x_j)$ recursively. Assume $M(x_i)$ has been defined for $i < j$ and consider the columns A, C and D in the submatrix $M_2(j)$. Replace column

$$A \text{ by} \begin{bmatrix} 1 \\ x_j \\ x_j \end{bmatrix}, \quad C \text{ by} \begin{bmatrix} 1 \\ 0 \\ x_j^2 \end{bmatrix}, \quad D \text{ by} \begin{bmatrix} 1 \\ x_j \\ 1 \end{bmatrix}$$

and call these replacements A_j, C_j and D_j respectively. (Column B (which is column a_2 of the submatrix M_1) is unchanged.) Then $E_j - L_j$ are determined uniquely as in Figure 3.2. For example, column F_j is on the line $\overline{a_2C_j}$ and $\overline{A_jD_j}$, so

$$F_j = \begin{bmatrix} 1 \\ x_j \\ x_j^2 \end{bmatrix}.$$

The others follow similarly. We note, as mentioned above, that G_j and J_j may *not* have been uniquely determined when $j > 1$. To accomplish this, we add two points, Q_j and P_j, to $M(x_j)$ when $j > 1$ as follows: Q_j is on $\overline{a_1A_j}$ and $\overline{a_5E_j}$ and P_j is on $\overline{C_{j-1}C_j}$ and $\overline{F_{j-1}F_j}$ (see Figure 3.2). In addition, we add column P_1 to $M(x_n)$ where P_1 is determined by $\overline{a_3C_n} \cap \overline{a_7F_n}$. Further, since H_j can be uniquely derived without the points Q_j and G_j precisely when $|r_j| \leqslant 1$, we delete columns Q_j and G_j from $M(x_j)$ when $|r_j| \leqslant 1$; otherwise, we leave them in. Finally, add L_1' to $M(x_1)$ if $\bar{b}_2 = 3$, where L_1' is on $\overline{a_2C_1}$ and $\overline{D_1K_1}$. (L_1' corresponds to

$$\begin{bmatrix} 0 \\ 1 \\ 2 \end{bmatrix}$$

in $M_2(1)$.)

We put Parts 1 and 2 together to define the matrix $M(N) = [M_1M(x_1)M(x_2) \cdots M(x_n)]$. Then $M(N)$ is a $3 \times K$ matrix, where $K \approx 14 \cdot \log_2 N + 9D \cdot k + 9$. Thus, in $M(N)$, given our (unjustified) choices for A_j, C_j and D_j, our remaining coordinates are uniquely determined. After our earlier concern about sequential uniqueness, the reader may be distressed by the obvious lack of same above. We remark, however, that we can still determine the characteristic set (of the derived configuration) by simply examining subdeterminants of $M(N)$. This follows from the fact that no numerical values have been assigned gratuitously in $M(N)$, i.e., if some subdeterminant is zero (or nonzero) over a field F, this reflects an actual dependence (or independence) encountered in trying to embed the derived configuration in $PG(2, F)$.

THEOREM 3.3. *Suppose* $6D \cdot k < p_1 < \cdots < p_k$ *and let* $C(N)$ *be the configuration arising from the column dependences of* $M(N)$ *over the prime* p_1. *Then* $\chi(C(N)) = \{p_1, \ldots, p_k\}$.

PROOF. We first show that $\chi(C(N)) \subseteq \{p_1, \ldots, p_k\}$. Now the three columns $L_1L_nP_1$ (or $L_1'L_nP_1$ if $\bar{b}_2 = 3$) have determinant equal to

$$\begin{vmatrix} 2 & N & 1 \\ x_1 & x_n & 0 \\ 2x_1^2 & Nx_n^2 & -x_1x_n \end{vmatrix} = (N-2)x_1x_n(x_1 + x_n) = p_1 \cdots p_K \cdot x_1x_n(x_1 + x_n).$$

Thus L_1 (or L_1'), L_n and P_1 are collinear in $C(N)$ (since p_1 divides this determinant). Since the factor of $p_1 \cdots p_k$ is uniquely determined (see arguments preceding Theorem 3.3), these three points will be independent over characteristic p for $p \neq p_i$, $1 \leqslant i \leqslant k$. Thus $\chi \subseteq \{p_1, \ldots, p_k\}$.

It remains to show the reverse inclusion. This requires a systematic check of all subdeterminants. For each $2 \leqslant m \leqslant k$, we must show the column dependences of $M(N)$ are exactly the same over p_m as they are over p_1. Now since each $p_m > 6D \cdot k$, any subdeterminant in which no $\bar{b}_i$ term appears will remain the same when considered modulo the respective primes (as $6D \cdot k \geqslant$ the absolute value of some coefficient in any such subdeterminant). Therefore, it suffices to consider only those subdeterminants which involve at least one of J_i, K_i, or L_i.

Case 1. *Subdeterminants in which all three columns are in one* $M(x_i)$. These correspond to "coded" versions of the subdeterminants of $M(i)$ from §2. For example, $\det(D_i G_i L_i) = (x_i^3 - x_i) \cdot S$, where S is the corresponding subdeterminant in $M(i)$. By construction of the $\bar{b}_i$ sequence and since x_i is transcendental, these subdeterminants cause no trouble. If P_i or Q_i is in our subdeterminant, see Case 2.

Case 2. *Not all three columns are in any* $M(x_i)$. We sketch the proof of Case 2. A more detailed analysis of such subdeterminants is left to the reader.

First note that any 3×3 subdeterminant not containing any P_i or Q_i will simply be a polynomial in $x_1, \ldots, x_n$ with at least one nonzero coefficient. For example,

$$\det(J_i A_j a_{3r+5}) = \begin{vmatrix} \bar{b}_i & 1 & 1 \\ x_i & x_j & r \\ \bar{b}_i x_i^2 & x_j & 0 \end{vmatrix} = r\bar{b}_i x_i^2 + x_i x_j - \bar{b}_i x_i^2 x_j - r\bar{b}_i x_j$$

is never zero modulo any of $p_1, \ldots, p_k$.

Including P_i may give rise to a subdeterminant of the form $f(\bar{b}_r, \bar{b}_s) \cdot g(x_i, x_j)$ for nonconstant polynomials f and g. But this subdeterminant can only occur when $j = i - 1$ and $|r - s| \leqslant 2$. This follows from the fact that points on the line $\overline{a_2 C_{i-1}}$ are projected onto the line $\overline{a_2 C_i}$ via P_i (see Figure 2.2). Thus our 3×3 subdeterminant above must contain one point on $\overline{a_2 C_{i-1}}$ and on $\overline{a_2 C_i}$. Evaluating the resulting determinants yields expressions which are zero over each p_m or nonzero over each p_m. For example, $\det(L_i P_i J_{i-1}) = x_i x_{i-1}(x_i + x_{i-1})(\bar{b}_{i+1} - \bar{b}_{i-1})$. But $\bar{b}_{i+1} - \bar{b}_{i-1}$ is a subdeterminant of $M(j)$ from §2, with $j = i + 1$, and so the construction of the $\bar{b}_i$ sequence precludes problems here.

The story is similar for the point Q_i, although slightly easier. In either case, any subdeterminant $S \equiv 0 \pmod{p_m}$ for some m will have $S \equiv 0 \pmod{p_m}$ for all m. This concludes our proof.

4. Finite prime-field characteristic sets. In Theorem 3.3, we note that although $\{x_1, \ldots, x_n\}$ were chosen to be transcendental, all that was needed was a guarantee that certain determinants involving these variables did not vanish. Indeed, the construction will remain valid as long as these variables do not satisfy any member of the finite list of polynomials arising from all the subdeterminants of $M(N)$. This observation leads to our main theorem.

THEOREM 4.1. *Suppose*

$$6D \cdot k < p_1 < \cdots < p_k < 2^{[(\sqrt{p_1} - Ak^{3/2})/Bk^{3/2}]} = f(p_1, k),$$

where A, B and D are fixed constants (independent of k, $p_1,\dots,p_k$) and p_1 is large enough so that there are (at least) k primes between p_1 and $f(p_1, k)$. Then $\{p_1,\dots,p_k\}$ forms a prime-field characteristic set.

PROOF. We construct the matrix $M(N)$ and the configuration $C(N)$ as in §3. Theorem 3.3 gives us $\chi(C(N)) = \{p_1,\dots,p_k\}$. We will show that $\chi_{pf}(C(N))$ exists (and equals $\{p_1,\dots,p_k\}$) by assigning prime-field values to each of $x_1,\dots,x_n$ so that no new dependences are created in $M(N)$ modulo any prime p_m $(1 \leqslant m \leqslant k)$.

We proceed recursively, assuming that values $c_1, c_2,\dots,c_{j-1}$ have been given to $x_1, x_2,\dots,x_{j-1}$, respectively, such that no new dependences have been created in the submatrix $(M_1M(c_1) \cdots M(c_{j-1}))$ mod p_m for any m (i.e., the 0-subdeterminants of $(M_1M(x_1) \cdots M(x_{j-1}))$ exactly match the 0-subdeterminants of $(M_1M(c_1) \cdots M(c_{j-1})))$.

Let R_j be the total number of positive integers less than p_1 which c_j cannot be. Then $R_j < R_n$ if $j < n$, for the selection of c_j involves avoiding the roots of fewer polynomials than the selection of c_n involves. (There are more subdeterminants in $(M_1M(c_1) \cdots M(c_{n-1})M(x_n))$ than in $(M_1M(c_1) \cdots M(c_{j-1}))$.) Thus it will be possible to assign prime-field integer values c_j to x_j for $1 \leqslant j \leqslant n$ if $R_n < p_1$. To compute R_n, we examine the subdeterminants of $M(N)$ which contain at least one column from $M(x_n)$ (where we assume $x_1 = c_1,\dots,x_{n-1} = c_{n-1}$).

There are $\binom{K}{3} - \binom{K-15}{3}$ such subdeterminants, where $K = |M(N)| \approx 14 \cdot \log_2 N + 9D \cdot k$, and each subdeterminant is (at most) a degree five polynomial in x_n. Then c_n cannot be any of the (at most) 5 roots for each subdeterminant and for each prime p_m. Hence, $R_n \leqslant 5k[\binom{K}{3} - \binom{K-15}{3}]$. Now

$$\binom{K}{3} - \binom{K-15}{3} \approx C_2 \cdot K^2 \approx C_2(\log_2 N + C_3 \cdot k)^2 \quad \text{for constants } C_2 \text{ and } C_3.$$

But $\log_2 N \leqslant k \cdot \log_2 p_k$, so we get $R_n \leqslant C_4k^3(\log_2 p_k + C_3)^2$.

Therefore, we can assign a value c_n to x_n (and hence c_j to x_j for all $j < n$) without introducing new dependences provided $C_4k^3(\log_2 p_k + C_3)^2 < p_1$, or $p_k < f(p_1, K)$ for constants $A = \sqrt{C_4} \cdot C_3$, $B = \sqrt{C}_4$.

To complete the proof, we need only check that, for k fixed and p_1 sufficiently large, there are k primes in the interval between p_1 and $f(p_1, k)$. But this follows easily from the Prime Number Theorem (see e.g., p. 371 of [**5**]). Thus, $\{p_1,\dots,p_k\}$ forms a prime-field set and we are done.

We note that any subset of a prime-field set formed in this fashion will also be a prime-field characteristic set. (Just apply the same construction to the subset.) This proves

COROLLARY 4.2. *For any $k > 0$, there are infinitely many prime-field characteristic sets containing exactly k primes.*

In general, it is unknown (and probably false) whether a subset of a finite prime-field characteristic set is again a prime-field characteristic set.

5. Cofinite prime-field characteristic sets. It is well known that $\{0\} \cup [p, \infty)_P$ forms a cofinite prime-field set for any prime p (where $[p, \infty)_P$ denotes the set of all primes $\geqslant p$). See **[2]** for details. We wish to determine what other forms cofinite sets can take. In particular, we show that certain finite sets of primes can be excluded from these "upper interval" cofinite sets.

Let n be a positive integer and let Q be an arbitrary set of k primes between n^2 and $n^2 + n$ (or $n^2 + n$ and $(n+1)^2$, resp.). Write $p_i = n^2 + r_i$ ($n^2 + n + r_i$, resp.) for each $p_i \in Q$, where $0 < r_i < n$ for all i.

Define the matrix $M(Q)$ to be

$$\begin{bmatrix} 1 & 0 & 0 & 1 & 1 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & & 1 & 0 & 1 & & 1 \\ 0 & 1 & 0 & 1 & 1 & 0 & 1 & -1 & 1 & 0 & 1 & 0 & 1 & \cdots & 0 & 1 & 0 & \cdots & 0 \\ 0 & 0 & 1 & 1 & 0 & 1 & 1 & 0 & -1 & 2 & -2 & 3 & -3 & & n & -n & -r_1 & & -r_k \end{bmatrix}$$

if the primes in Q are between n^2 and $n^2 + n$. If each $p_i \in Q$ is between $n^2 + n$ and $(n+1)^2$, we define $M'(Q)$ be deleting

$$\begin{bmatrix} 1 \\ n \\ 0 \end{bmatrix}$$

from $M(Q)$ and adding

$$\begin{bmatrix} 1 \\ 0 \\ n+1 \end{bmatrix} \quad \text{and} \quad \begin{bmatrix} 1 \\ n+1 \\ 0 \end{bmatrix}.$$

Let $C(Q)$ ($C'(Q)$, resp.) denote the matroid configuration arising from the column dependences of $M(Q)$ ($M'(Q)$, resp.) over the integers. We state Theorem 5.1 without proof.

THEOREM 5.1. (1) *$C(Q)$ ($C'(Q)$, resp.) is sequentially unique.*
(2) $\chi_{pf}(C(Q)) = \{0\} \cup [n^2, \infty)_P - Q$.
(3) $\chi_{pf}(C'(Q)) = \{0\} \cup [n^2 + n, \infty)_P - Q$.

Finally, we note that if there are k primes between n^2 and $n^2 + n$ (or $n^2 + n$ and $(n+1)^2$), Theorem 5.1 gives us 2^k prime-field sets, of which only $k + 1$ are upper interval sets.

REFERENCES

1. T. Brylawski, *Finite prime-field characteristic sets for planar configurations*, Linear Algebra Appl. **46** (1982), 155–176.

2. T. Brylawski and D. Kelly, *Matroids and combinatorial geometries*, Lecture Notes Ser., University of North Carolina, Chapel Hill, N. C., 1980.

3. T. Brylawski and D. Lucas, *Uniquely representable combinatorial geometries*, Proceedings of the International Colloquium on Combinatorial Theory, Rome, 1976, pp. 83–104.

4. G. Gordon, *Representations of matroids over prime fields*, Ph.D. Thesis, University of North Carolina, Chapel Hill, N. C., 1983.

5. G. Hardy and E. Wright, *An introduction to the theory of numbers*, Oxford Univ. Press, London, 1938, 1945, 1954, 1960, 1979.

6. A. W. Ingleton, *Representation of matroids*, Combinatorial Mathematics and its Applications (D. J. A. Welsh, ed.), Academic Press, New York, 1971, pp. 149–167.

7. J. Kahn, *Characteristic sets of matroids*, J. Loncon Math. Soc. (2) **26** (1982), 207–217.

8. R. Rado, *Note on independence functions*, Proc. London Math. Soc. (3) **7** (1957), 300–320.

9. R. Reid, *Obstructions to representations of combinatorial geometries* (unpublished; appears as Appendix in [**2**]).

10. W. Tutte, *Lectures on matroids*, J. Res. Nat. Bur. Standards **69B** (1965), 1–47.

11. P. Vamos, *A necessary and sufficient condition for a matroid to be linear*, Matroid Conf. (Brest, 1970).

12. S. S. Wagstaff, Jr., *Infinite matroids*, Trans. Amer. Math. Soc. **175** (1973), 141–153.

DEPARTMENT OF MATHEMATICAL SCIENCES, WILLIAMS COLLEGE, WILLIAMSTOWN, MASSACHUSETTS 01267