Quadratic Nonresidues and the Combinatorics of Sign Multiplication

Steve Wright
Department of Mathematics and Statistics
Oakland University
Rochester, MI 48309-4485
U.S.A.

Abstract

Let S be a finite, nonempty set of nonzero integers which contains no squares. We obtain conditions both necessary and sufficient for S to have the following property: for infinitely many primes p, S is a set of quadratic nonresidues of p. The conditions are expressed solely in terms of purely external (respectively, internal) combinatorial properties of the set Π of all prime factors of odd multiplicity of the elements of S. We also calculate by means of certain purely combinatorial parameters associated with Π the density of the set of all primes p such that S is a set of quadratic residues of p and the density of the set of all primes p such that S is a set of quadratic nonresidues of p.

1 Introduction

If Z^+ denotes the set of positive integers and $p \in Z^+$ is an odd prime, an integer z is a *quadratic residue* (respectively, *quadratic nonresidue*) *of* p if $x^2 \equiv z \bmod p$ has (respectively, does not have) an integer solution x. Quadratic residues and nonresidues have been of considerable interest in number theory almost from the very beginning of that subject as a serious mathematical discipline, starting with the work of Euler and becoming of major importance when Gauss made them a central topic of the *Disquisitiones Arithmeticae* (see [1, 9] for good historical reviews of work on quadratic residues). In [14], motivated by work of Buell and Hudson [2], Fi-

laseta and Richman [4] (see also Fried [5] on more general power residues, of which some of the results of [4] are special cases), Hudson [8], and Monzingo [10], we began a study of the following problem: characterize the nonempty finite subsets S of Z^+ such that for infinitely many primes p, every element of S is a quadratic residue (respectively, quadratic nonresidue) of p. The solution to this problem for quadratic residues turned out to be simple, both in statement and proof: *every* nonempty finite subset of Z^+ is a set of quadratic residues for infinitely many primes ([14, Theorem 2.3]).

The corresponding problem for quadratic nonresidues, however, is much more subtle. Its solution is well-known and classical; we have included it in the statement of Theorem 2.14, section 2, the equivalence of conditions (i) and (ii) of that theorem. A proof of this can be obtained by straightforwardly modifying a clever argument using the Dedekind zeta function due to Hilbert [7, Satz 111] (cf. Hecke [6, Satz 147]; this argument, in fact, goes all the way back to Dirichlet [3]). Fried [5, Corollary III.A] appears to have given the first published elementary proof, and a refined version of this solution was discovered by Fileseta and Richman [4, Theorem 1], who gave three different proofs. Schinzel [12] extended Fried's results to power residues in arbitrary algebraic number fields; Schinzel and Skalba [13] have obtained the most general results along these lines. In the present paper, however, we take a different tack. We find solutions that are expressed solely by purely internal and external combinatorial conditions satisfied by the set of prime factors of odd multiplicity of the elements of S. Because of this, our main results for number theory (the equivalence of statements (i) and (iv) in Theorem 2.12, the equivalence of statements (i), (iii), (iv), and (v) in Theorem 2.14, and Theorems 3.3 and 3.4) do not appear to be deducible in a reasonable manner from results in [5], [12], and/or [13].

We now formulate a more precise version of this problem that emphasizes our combinatorial approach to it. For $z \in Z^+$, denote by $\pi_{\text{odd}}(z)$ the set of all prime factors of z of odd multiplicity. It can be shown ([14, Lemmas 2.1 and 2.4]) that if S is a nonempty, finite subset of Z^+ which contains no squares and if Π is the set of all prime factors of the elements of S of odd multiplicity, then S is a set of quadratic nonresidues for infinitely many primes if and only if

(*) there exists a subset N of Π such that for all $z \in S$, the cardinality of $N \cap \pi_{\text{odd}}(z)$ is odd.

Our problem can now be reformulated as follows: characterize the finite nonempty, square-free subsets of Z^+ for which condition (*) holds. When viewed this way, one immediately realizes that quadratic nonresidues no

longer play any role; instead, a purely combinatorial problem about sets of subsets of a fixed finite set becomes the main issue.

Thus, if A is a nonempty finite set, if 2^A denotes the set of all subsets of A, if $\emptyset$ denotes the empty set, and if $\emptyset \neq \mathcal{S} \subseteq 2^A \backslash \{\emptyset\}$ then we will say that $\mathcal{S}$ has the *odd-intersection property* (with respect to A) if there exits a subset N of A such that for all $S \in \mathcal{S}$ the cardinality of $N \cap S$ is odd. It is easy to see that $\mathcal{S}$ has the odd-intersection property with respect to A if and only if there is a choice of signs $\epsilon : A \to \{-1, 1\}$ such that

$$\prod_{a \in S} \epsilon(a) = -1, \text{ for all } S \in \mathcal{S}.$$

This is why we consider the odd-intersection property as a concept in the "combinatorics of sign multiplication."

The reformulation of our original quadratic nonresidue problem in terms of the odd-intersection property is important enough to record formally in the following lemma:

Lemma 1.1 *If S is a nonempty finite subset of Z^+ which contains no squares and if Π is the set of all prime factors of the elements of S of odd multiplicity, then S is a set of quadratic nonresidues for infinitely many primes if and only if $\{\pi_{\text{odd}}(z) : z \in S\}$ has the odd-intersection property with respect to Π.*

Lemma 1.1 now focuses our attention on what we will call

> *The basic problem:* if A is a nonempty finite set and $\emptyset \neq \mathcal{S} \subseteq 2^A \backslash \{\emptyset\}$, find a good characterization of the odd-intersection property for $\mathcal{S}$ with respect to A.

By a "good" characterization here, we mean one that involves only the set-theoretic structure of $\mathcal{S}$, and which, in particular, avoids dependence on the subset N that appears in the definition of the odd-intersection property.

In [14], we were able to solve the basic problem when $\mathcal{S}$ has at most four elements ([14, Proposition 3.3]), and we left the general case of the basic problem open as a topic of further research ([14, section 4, problem (1)]). As occurs frequently in combinatorics, our solution there asserted that the odd-intersection property was guaranteed precisely for $\mathcal{S}$ by the avoidance of the inclusion in $\mathcal{S}$ of certain explicitly constructed set-theoretic obstructions (the 2-cycles of type 1 and the 3-cycles of type 2 defined in section 2

infra). The first main result of the paper before the reader (Theorem 2.11, section 2) presents a solution of the basic problem in the general case along these same lines. The second main result (Theorem 2.13, section 2) gives an internal characterization of the odd-intersection property in terms of repeated symmetric differences of elements of subsets of odd cardinality. The third main result (Theorem 2.12, section 2), essentially a corollary of our solutions to the basic problem, provides the anticipated characterization of the finite subsets of Z^+ that are sets of quadratic nonresidues for infinitely many primes. Two interesting problems in enumerative combinatorics naturally arise from our solution to the basic problem, and we hence discuss these briefly at the end of section 2. Finally, motivated by the results of section 2 and a result of [14], we calculate in section 3 the density of the set of primes with a fixed finite set of quadratic residues or a fixed finite set of quadratic nonresidues.

2 Solution of the basic problem

If $n \in Z^+$, then $[1,\ n]$ will denote the n-set $\{1, \ldots, n\}$; more generally, if $m, n \in Z^+$, $2 \leq m \leq n$, then $[m, n]$ will denote the set of all elements of $[1,\ n]$ that exceed $m-1$. If A is a set, then $|A|$ will denote the cardinality of A. Let $n \geq 2$ be a positive integer fixed throughout the remainder of this section.

A nonempty subset $\mathcal{S}$ of $2^{[1,\ n]} \backslash \{\emptyset\}$ is an *obstruction to the odd-intersection property*, or more succinctly, an *obstruction*, if $\mathcal{S}$ does not have the odd-intersection property, but all nonempty proper subsets of $\mathcal{S}$ do have it. Obstructions are of interest to us because of the following simple fact:

Lemma 2.1 *A nonempty subset of* $2^{[1,\ n]} \backslash \{\emptyset\}$ *has the odd-intersection property if and only if it does not contain an obstruction.*

We can hence solve the basic problem if we can determine the structure of the obstructions in $2^{[1,\ n]}$ in an explicit enough way.

A class of obstructions with a particularly simple structure is given by the set of m-cycles of odd cardinality. Let $m \geq 2$ be an integer and let $\{V_1, \ldots, V_m\} \subseteq 2^{[1,\ n]} \backslash \{\emptyset\}$ with $V_i \cap V_j = \emptyset$ for $i \neq j$. An *m-cycle* is a set of the form

$$\left\{ V_1, \ldots, V_m, \bigcup_1^m V_i \right\}$$

(an m-cycle of *type 1*) (if $m \geq 2$) or of the form

$$\{V_1 \cup V_2,\ V_2 \cup V_3, \ldots,\ V_{m-1} \cup V_m,\ V_1 \cup V_m\}$$

(an m-cycle of *type 2*) (if $m \geq 3$). *N.B.* This definition of m-cycle differs slightly from the definition of m-cycle given in [13]. It is easy to see that an m-cycle is an obstruction if and only if its cardinality is odd and one can show that every obstruction of cardinality 3 is either a 2-cycle of type 1 or a 3-cycle of type 2.

Now, let $F = \{0, 1\}$ denote the Galois field $Z/2Z$ of order 2, and let F^n denote the vector space of dimension n over F. We will use linear algebra in F^n to study obstructions in $2^{[1,n]}$ by means of the following familiar device. If $S \subseteq [1, n]$, we associate a vector $v_S \in F^n$ to S by defining the i-th coordinate $v_S(i)$ of v_S to be 0 (respectively, 1) if $i \notin S$ (respectively, $i \in S$). Note that the map $S \to v_S$ is a bijection of $2^{[1,n]}$ onto F^n. If $u, v \in F^n$ and we let $(u, v) = \sum_i u(i)v(i)$ denote the standard inner product of u and v over F, then the following lemma is evident:

Lemma 2.2 *If N and S are subsets of $[1, n]$, then $|N \cap S|$ is odd if and only if $(v_N, v_S) = 1$ in F.*

By means of Lemma 2.2, we can transfer the analysis of obstructions in $2^{[1,n]}$ to the analysis of certain subsets of F^n which we describe next. If $V \subseteq F^n$ and $v \in V$, then we will say that v is *separated from the other elements of* V if there exists $x \in F^n$ such that

$$0 = (x, v) \text{ and } 1 = (x, w),\ \forall w \in V \backslash \{v\}.$$

The vector x is said to *separate v from the other elements of V*. We declare that V has *property* (a) if for each $x \in F^n$, there exists $v \in V$ such that $0 = (x, v)$, that V has *property* (b) if each element of V is separated from the other elements of V, and that V is an *obstruction in F^n* if $0 \notin V$ and V has properties (a) and (b). It is now a consequence of Lemma 2.2 and these definitions that we have

Lemma 2.3 *If $\mathcal{S} \subseteq 2^{[1,n]}$ and $V_{\mathcal{S}} = \{v_S : S \in \mathcal{S}\}$, then $\mathcal{S}$ is an obstruction in $2^{[1,n]}$ if and only if $V_{\mathcal{S}}$ is an obstruction in F^n.*

We hence turn our attention to obstructions in F^n.

Lemma 2.4 *The cardinality of an obstruction in F^n must be odd and at least* 3.

Proof. Let $\mathcal{O} = \{w_1, \ldots, w_m\}$ be an obstruction in F^n of cardinality m. It is clear that $\mathcal{O}$ cannot be a singleton. If x_i separates w_i from the other elements of $\mathcal{O}$, then

$$\left(\sum_1^m x_k, w_i\right) = (m-1) \cdot 1, i \in [1, m].$$

Hence if $m-1$ is odd,

$$\left(\sum_1^m x_k, w\right) = 1, \ \forall w \in \mathcal{O},$$

contradicting the fact that $\mathcal{O}$ has property (a). Thus $m-1$ is even, i.e., m is odd. QED

We will study obstructions in F^n by means of their incidence matrices, which are defined in the usual way as follows: if $V = \{v_1, \ldots, v_m\} \subseteq F^n \backslash \{0\}$, the *incidence matrix* $I(V)$ *of* V is defined to be the $m \times n$ matrix over F whose (i,j) entry is $v_i(j)$. Since $0 \notin V$, every row of $I(V)$ is nonzero, and the number of rows of $I(V)$ agrees with the cardinality of V.

Properties (a) and (b) , the defining properties of an obstruction, have an equivalent formulation in terms of properties of the incidence matrix. Let $V \subseteq F^n \backslash \{0\}$, with $m = |V| > 0$, and let $\{e_1, \ldots, e_m\}$ be the standard basis of F^m, i.e., for each i and j, $e_j(i) = \delta_{ij}$, where δ_{ij} denotes the Kronecker delta. Then

(i) V has property (a) if and only if for all vectors y in the column space of $I(V)$, there exists $i \in [1, m]$ such that $y(i) = 0$, and

(ii) V has property (b) if and only if for all $i \in [1, m]$, $\sum_{j \neq i} e_j$ is in the column space of $I(V)$.

Now let $\mathcal{O}$ be an obstruction in F^n, with $m = |\mathcal{O}|$. Consider

$$\mathcal{Y}_{m-1} = \text{the subspace of } F^m \text{ consisting of all vectors with an } \textit{odd} \text{ number of 0 coordinates.}$$

We observe that $\mathcal{Y}_{m-1}$ is the linear span over F of

$$\left\{\sum_{j \neq i} e_j : \ i \in [1, m]\right\}$$

and has dimension $m-1$ over F (a basis of $\mathcal{Y}_{m-1}$ is $\{e_i + e_m : i \in [1,m-1]\}$) Since $\mathcal{O}$ has property (b), it follows from observation (ii) that

$$\mathcal{Y}_{m-1} \subseteq \text{ column space of } I(\mathcal{O}) \subseteq F^m,$$

and since $\mathcal{O}$ has property (a), it follows from observation (i) that

$$\sum_1^m e_i \notin \text{ column space of } I(\mathcal{O}).$$

We conclude that

$$\mathcal{Y}_{m-1} = \text{ column space of } I(\mathcal{O}).$$

Conversely, if $V \subseteq F^n \backslash \{0\}$ has odd cardinality $m \geq 3$ and the column space of $I(V)$ is $\mathcal{Y}_{m-1}$, then every element of the column space of $I(V)$ has at least one 0 coordinate, and for all $i \in [1,m]$, $\sum_{j \neq i} e_j$ is in the column space of $I(V)$. Thus by observations (i) and (ii), V is an obstruction. We have hence established

Lemma 2.5 *If V is a subset of $F^n \backslash \{0\}$ of odd cardinality $m \geq 3$, then V is an obstruction if and only if the column space of $I(V)$ is $\mathcal{Y}_{m-1}$, the subspace of F^m consisting of all vectors with an odd number of 0 coordinates.*

We next describe two procedures which produce (perhaps) new obstructions from old ones. This will require some additional terminology associated with subsets of F^n. If $v \in F^n$, then the *support* $\Sigma(v)$ *of* v is the subset of $[1,n]$ defined by

$$\Sigma(v) = \{i : v(i) = 1\}.$$

If $\emptyset \neq V \subseteq F^n$, the *support* $\Sigma(V)$*of* V is defined to be

$$\Sigma(V) = \bigcup_{v \in V} \Sigma(v).$$

Note that the nonzero columns of $I(V)$ are precisely the columns $\begin{pmatrix} v_1(i) \\ \vdots \\ v_{|V|}(i) \end{pmatrix}$ for which $i \in \Sigma(V)$. We say that V is *nondegenerate* if $\Sigma(V) = [1,n]$ and that V is *essential* if the nonzero columns of $I(V)$ are all distinct and linearly independent over F.

If follows from observation (i) above that if $\emptyset \neq V \subseteq F^n$ has property (a), if each column from a submulti-set of columns of $I(V)$ is replaced in $I(V)$ by a column of 0's, and if V' is the subset of F^n with the resulting incidence matrix, then V' also has property (a). (In the course of replacing columns of $I(V)$ by columns of 0's, repeated rows may occur, all but one in each occurence of which must be deleted in forming $I(V')$. This construction may also produce $V' = \{0\}$, which for technical reasons was not included in our definition of the incidence matrix, but this will cause no difficulties). It also follows from observation (ii) above that if V has property (b), if B is a subset of columns of $I(V)$ which form a basis for the column space of $I(V)$, if the columns of $I(V)$ not in B (if any) are replaced by columns of 0's, and if V' is the subset of F^n with the resulting incidence matrix, then V' has property (b).

Now, let $\mathcal{O} \subseteq F^n$ be an obstruction.

Reduction to an essential obstruction

Let B be a subset of the columns of $I(\mathcal{O})$ which form a basis of the column space of $I(\mathcal{O})$, replace the columns of $I(\mathcal{O})$ not in B (if any) by columns of 0's, and let $\mathcal{O}'$ be the subset of F^n with the resulting incidence matrix. It is then a consequence of our remarks in the preceding paragraph that $\mathcal{O}'$ is an essential obstruction in F^n.

Expansion to a nondegenerate obstruction

If $\mathcal{O}$ is degenerate, replace all the zero columns in $I(\mathcal{O})$ by any multi-set of nonzero elements from the column space of $I(\mathcal{O})$, and let $\mathcal{O}'$ be the subset of F with the resulting incidence matrix. Then $\mathcal{O}'$ is nondegenerate and the column space of $I(\mathcal{O}')$ = the column space of $I(\mathcal{O})$, hence by Lemma 2.5, $\mathcal{O}'$ is an obstruction.

It is clear that if $\mathcal{O}$ is a nondegenerate essential obstruction, then reduction to an essential obstruction or expansion to a nondegenerate obstruction applied to $\mathcal{O}$ will produce nothing new. The nondegenerate essential obstructions can hence be considered as irreducible objects viz a viz the odd-intersection property, and can therefore be expected to play a key role in the determination of the structure of an arbitrary obstruction.

Lemma 2.6 *If $\mathcal{O} \subseteq F^n$ is a nondegenerate, essential obstruction, then n is even and $|\mathcal{O}| = n + 1$.*

Proof. The cardinality $|\mathcal{O}|$ of $\mathcal{O}$ is odd by Lemma 2.4, and the rank of $I(\mathcal{O})$ is $|\mathcal{O}| - 1$ by Lemma 2.5. Since $\mathcal{O}$ is nondegenerate and essential, the rank of $I(\mathcal{O})$ must also be n. Hence $n = |\mathcal{O}| - 1$ and n is even. QED

Proposition 2.7 *If $n \geq 2$ is an even (respectively, odd) integer, then the cardinality of an obstruction in F^n is an odd integer in $[3,\ n+1]$ (respectively, $[3,\ n]$). Moveover, every odd integer in this interval occurs as the cardinality of an obstruction in F^n.*

Proof. Let $\mathcal{O}$ be an obstruction in F^n with $m = |\mathcal{O}|$. By reduction to an essential obstruction starting with $\mathcal{O}$, we find an essential obstruction $\mathcal{O}'$ such that the column space of $I(\mathcal{O}')$ contains $\sum_{j \neq i} e_j$ for $i \in [1, m]$, where $\{e_1, \ldots, e_m\}$ is the standard basis of F^m. It follows that $I(\mathcal{O}')$ must have m distinct rows, all of which are nonzero. Since the number of rows in an incidence matrix counts the cardinality of the underlying set, we conclude that $|\mathcal{O}| = |\mathcal{O}'|$. Since $\mathcal{O}'$ is essential and nondegenerate on its support $\Sigma(\mathcal{O}')$, it follows from Lemma 2.6 that $|\Sigma(\mathcal{O}')|$ is an even integer in $[2, n]$ (respectively, $[2, n-1]$) if n is even (respectively, odd) and that $|\mathcal{O}'| = 1 + |\Sigma(\mathcal{O}')|$. Hence $|\mathcal{O}| = |\mathcal{O}'|$ is an odd integer in $[3, n+1]$ (respectively, $[3, n]$) if n is even (respectively, odd). Conversely, if m is an even integer in $[2, n]$ and if $\mathcal{S}$ is an m-cycle of type 1 contained in $2^{[1,n]}$, then $V_{\mathcal{S}}$ is a obstruction in F^n of cardinality $m+1$. QED

If n is even (respectively, odd) and m is an odd integer in $[3, n+1]$ (respectively, $[3, n]$), then we let $\mathcal{O}_m(n)$ denote the set of all obstructions in F^n of cardinality m. We can now systematically generate the elements of $\mathcal{O}_m(n)$ as follows. Let $S \subseteq [1, n]$ be a set of cardinality $m-1$ and let B be a basis of $\mathcal{Y}_{m-1}$. Let $\mathcal{O}(S, B)$ denote any essential obstruction in F^n with support S and with incidence matrix $I(S, B)$ whose nonzero columns are precisely the elements of B. Then $\mathcal{O}(S, B) \in \mathcal{O}_m(n)$, and if $\mathcal{O}$ is any subset of F^n whose incidence matrix is obtained from $I(S, B)$ by replacing a set of zero columns of $I(S, B)$ (if any) by a multi-set of column vectors from $\mathcal{Y}_{m-1}$, then $\mathcal{O} \in \mathcal{O}_m(n)$. Conversely, every element of $\mathcal{O}_m(n)$ is obtained in this way from a subset S of $[1, n]$ of cardinality $m-1$, a basis B of $\mathcal{Y}_{m-1}$, and a multi-set of column vectors from $\mathcal{Y}_{m-1}$.

The task now before us is to transfer the above results on obstructions in F^n to results on obstructions in $2^{[1,n]}$. This is, of course, carried out by means of the bijection of $2^{[1,n]}$ onto F^n we defined previously. Thus, if $\emptyset \neq \mathcal{S} \subseteq 2^{[1,n]} \backslash \{\emptyset\}$, we define the *incidence matrix* $I(\mathcal{S})$ of $\mathcal{S}$ to be $I(V_{\mathcal{S}})$ and the *column set* $C(\mathcal{S})$ *of* $\mathcal{S}$ to be the set of all nonzero columns of $I(\mathcal{S})$. Note that $C(\mathcal{S}) \subseteq F^m$, where $m = |\mathcal{S}|$. From Lemmas 2.3 and 2.5, we readily deduce

Lemma 2.8 *If $\emptyset \neq \mathcal{S} \subseteq 2^{[1,n]} \backslash \{\emptyset\}$ and $m = |\mathcal{S}|$ is odd and at least 3, then $\mathcal{S}$ is an obstruction in $2^{[1,n]}$ if and only if the column space of $I(\mathcal{S})$ is $\mathcal{Y}_{m-1}$.*

We also note that Proposition 2.7 remains true when obstructions in F^n are replaced there by obstructions in $2^{[1,n]}$.

As is evident from Lemma 2.8, only the column set of $\mathcal{S}$ determines whether or not $\mathcal{S}$ is an obstruction. We hence desire a way of expressing the elements of $\mathcal{S}$ which exposes the manner in which the column set of $\mathcal{S}$ determines the set-theoretic structure of the elements of $\mathcal{S}$. This is afforded by the well-known atomic decomposition of a class of sets, which we now describe.

Let $\emptyset \neq \mathcal{S} \subseteq 2^{[1,n]} \backslash \{\emptyset\}$, with $m = |\mathcal{S}|$, and let $c_1, \ldots, c_n$ denote the columns of $I(\mathcal{S})$. Define an equivalence relation $\sim$ on $[1,n]$ as follows: if $(i,j) \in [1,n] \times [1,n]$, then $i \sim j$ if $c_i = c_j$. *N. B.* This equivalence relation is invariant under permutation of the rows of $I(\mathcal{S})$. Let E_0 denote the equivalence class determined by the zero columns of $I(\mathcal{S})$, if any, and set

$$A(\mathcal{S}) = \text{set of all distinct equivalence classes of } \sim, \textit{excluding } E_0.$$

Then $A(\mathcal{S}) \neq \emptyset$ and there is a bijection $b_{\mathcal{S}} : C(\mathcal{S}) \to A(\mathcal{S})$ of $C(\mathcal{S})$ onto $A(\mathcal{S})$ such that if

$$S_i = \bigcup_{\{c \in C(\mathcal{S}):\, c(i)=1\}} b_{\mathcal{S}}(c),\ i \in [1,m], \tag{2.1}$$

then $\mathcal{S} = \{S_1, \ldots, S_m\}$. The elements of $A(\mathcal{S})$ are the *atoms of* $\mathcal{S}$, the bijection $b_{\mathcal{S}}$ is the *attachment map of* $\mathcal{S}$, and the decomposition (2.1) is the *atomic decomposition of* $\mathcal{S}$.

A nonempty set C of column vectors in F^m is *admissible* if C is non-degenerate and for $i \neq j$, there exists $c \in C$ such that $c(i) \neq c(j)$. If $m \in [1, 2^n]$, $k \in [1,n]$, A is a subset of $2^{[1,n]} \backslash \{\emptyset\}$ of cardinality k whose elements are pairwise disjoint, C is an admissible set of nonzero column vectors in F^m of cardinality k, $b : C \to A$ is a bijection , and

$$S_i = \bigcup_{\{c \in C:\, c(i)=1\}} b(c),\ i \in [1,m],$$

then $\mathcal{S} = \{S_1, \ldots, S_m\}$ is a subset of $2^{[1,n]} \backslash \{\emptyset\}$ of cardinality m with column set C, atoms A, and attachment map b.

If one now considers the 0-1 matrix formed by the column vectors in the column set of a nonempty subset $\mathcal{S}$ of $2^{[1,n]} \backslash \{\emptyset\}$, the atomic decomposition of $\mathcal{S}$ reveals how this matrix displays the pattern formed by the intersections of the elements of $\mathcal{S}$. This observation motivates what we do next.

If X and Y are arbitrary matrices, we will say that X is *permutation-equivalent to* Y if X is obtained from Y by permutation of the rows and

columns of Y. If we call the set of all columns of a matrix X the *column set of* X, we note that if X and Y have distinct columns, then X is permutation-equivalent to Y if and only if X and Y have the same size and there exists a permutation of the coordinates of the column space of Y which sends the column set of Y onto the column set of X. Since permutation equivalence is obviously an equivalence relation on the set of all matrices over a fixed field, we will let $[X]$ denote the associated equivalence class of the matrix X.

If $\mathcal{S}$ is now a nonempty subset of $2^{[1,n]}\backslash\{\emptyset\}$, let X be any matrix of size $|\mathcal{S}| \times |C(\mathcal{S})|$ whose column set is $C(\mathcal{S})$ (note that X has distinct rows and columns). The *intersection pattern of* $\mathcal{S}$ is defined to be $[X]$, and this definition clearly does not depend on how X is formed from an ordering of the elements of $C(\mathcal{S})$. Two nonempty subsets of $2^{[1,n]}\backslash\{\emptyset\}$ are said to be *pattern equivalent* if they have the same intersection pattern.

Lemma 2.9 *If $\emptyset \neq \mathcal{S} \subseteq 2^{[1,n]}\backslash\{\emptyset\}$, then $\mathcal{S}$ is an obstruction if and only if $\mathcal{S}$ is pattern equivalent to an obstruction.*

Proof. If $\mathcal{S}$ is pattern equivalent to an obstruction $\mathcal{O}$, then $|\mathcal{S}| = m = |\mathcal{O}|$ and there is a permutation π of the coordinates of F^m such that $\pi(C(\mathcal{O})) = C(\mathcal{S})$. Because $\mathcal{O}$ is an obstruction,

$$\text{span over } F \text{ of } C(\mathcal{O}) = \text{ column space of } I(\mathcal{O}) = \mathcal{Y}_{m-1}.$$

But $\mathcal{Y}_{m-1}$ is invariant under any permutation of the coordinates of F^m, and so

$$\begin{aligned} \text{column space of } I(\mathcal{S}) &= \text{ span over } F \text{ of } C(\mathcal{S}) \\ &= \pi(\text{span over } F \text{ of } C(\mathcal{O})) \\ &= \pi(\mathcal{Y}_{m-1}) \\ &= \mathcal{Y}_{m-1}. \end{aligned}$$

We hence conclude from Lemma 2.8 that $\mathcal{S}$ is an obstruction. QED

We now describe a class of intersection patterns that will play a decisive role in our solution of the basic problem. Let $n \geq 2$ be an integer, let m be an odd integer in $[3, n+1]$ (respectively, $[3, n]$) if n is even (respectively, odd], and let $k \in [m-1, \min\{2^{m-1}-1, n\}]$. We set

$$\mathcal{C}_{mk}(n) = \{C \subseteq \mathcal{Y}_{m-1} \setminus \{0\} : \ |C| = k \text{ and } C \text{ contains a basis of } \mathcal{Y}_{m-1}\}$$

and declare an intersection pattern $[X]$ to be *forbidden* if there exist n, m, and k as specified above such that X is of size $m \times k$ and the column set

of X is an element of $\mathcal{C}_{mk}(n)$. For each n, m, and k as specified, we let $\mathcal{F}_{mk}(n)$ denote the set of all forbidden intersection patterns of size $m \times k$.

There is a parameterization of $\mathcal{F}_{mk}(n)$ which makes the structure of forbidden intersection patterns even more transparent. In order to describe it, we first consider subsets U and V of F^m and declare them to be *permutation-equivalent* if there exists a permutation π of the coordinates of F^m such that $\pi(U) = V$. This is clearly an equivalence relation and we let $\langle U \rangle$ denote the associated equivalence class of $U \subseteq F^m$. Upon observing that $\mathcal{C}_{mk}(n)$ is invariant under any permutation of the coordinates of F^m, the following proposition is now evident from the construction of forbidden intersection patterns given above:

Proposition 2.10 *If $n \geq 2$ is an even (respectively, odd) integer, if m is an odd integer in $[3, n+1]$ (respectively, $[3, n]$) and if*

$$k \in \left[m-1, \min\{2^{m-1}-1, n\}\right],$$

then there is a bijection of $\mathcal{F}_{mk}(n)$ onto the equivalence classes of $\mathcal{C}_{mk}(n)$ under permutation equivalence of subsets of F^m given by

$$[X] \rightarrow \langle \textit{column set of } X \rangle.$$

It is now a consequence of Lemma 2.9 and the construction of the elements of $\mathcal{O}_m(n)$ in the paragraph which immediately follows the proof of Lemma 2.7 that a nonempty subset of $2^{[1,n]} \setminus \{\emptyset\}$ is an obstruction if and only if it has a forbidden intersection pattern. We thus deduce from Lemma 2.1 the following result, which constitutes our first solution of the basic problem:

Theorem 2.11 *If n is a positive integer, then a nonempty subset $\mathcal{S}$ of $2^{[1,n]} \setminus \{\emptyset\}$ has the odd-intersection property if and only if $\mathcal{S}$ does not contain a subset of $2^{[1,n]}$ with a forbidden intersection pattern.*

Remark. If n, m, and k are specified as in Proposition 2.10, if $[X] \in \mathcal{F}_{mk}(n)$, and if $\mathcal{A} \subseteq 2^{[1,n]} \setminus \{\emptyset\}$ is a set of atoms with $|\mathcal{A}| = k$, then there is an algebraic algorithm which explicitly constructs all elements of $\mathcal{O}_m(n)$ with intersection pattern $[X]$ and set of atoms $\mathcal{A}$ ([16, Lemma 3.3]). Consequently, when this algorithm is combined with the atomic decomposition, we generate algorithmically and bijectively all obstructions in $2^{[1,n]}$.

There are various ways to transfer the results we have obtained so far from n-sets to arbitrary finite sets. In this more general situation, the main

issue is the formulation of an appropriate definition of intersection pattern. In the interest of completeness, we will now present a method for doing that.

Let A be a nonempty finite set, and let $\emptyset \neq \mathcal{S} \subseteq 2^A \backslash \{\emptyset\}$. We define an equivalence relation $\sim$ on A as follows: if $(a, b) \in A \times A$ then $a \sim b$ if for all $S \in \mathcal{S}$, $a \in S$ if and only if $b \in S$. Let $\mathcal{E}$ denote the set of distinct equivalence classes of $\sim$. If $E_0 = \{a \in A : a \notin S, \text{ for all } S \in \mathcal{S}\}$, then $E_0 \in \mathcal{E}$ if and only if $E_0 \neq \emptyset$. If we set $\mathcal{E}' = \mathcal{E} \backslash \{E_0\}$, then $\mathcal{E}' \neq \emptyset$ and it follows easily from the definition of $\sim$ that

$$S = \bigcup_{\{E \in \mathcal{E}' :\, S \cap E \neq \emptyset\}} E, \ \forall S \in \mathcal{S}.$$

This is, of course, just the "coordinate-free" version of the atomic decomposition of $\mathcal{S}$.

If $m = |\mathcal{S}|$, $k = |\mathcal{E}'|$, and if $\{S_1, \ldots, S_m\}$, $\{E_1, \ldots, E_k\}$ are enumerations of $\mathcal{S}$ and $\mathcal{E}'$, respectively, then we define the matrix $X(\mathcal{S}) = (x_{ij})$ of size $m \times k$ as follows:

$$x_{ij} = \begin{cases} 1, & \text{if } E_j \subseteq S_i \\ 0, & \text{if } E_j \cap S_i = \emptyset. \end{cases}$$

The *intersection pattern of* $\mathcal{S}$ is defined to be $[X(\mathcal{S})]$. The intersection pattern of $\mathcal{S}$ clearly does not depend on the enumerations of $\mathcal{S}$ and $\mathcal{E}'$ used to define $X(\mathcal{S})$, and it is also invariant under bijections, i.e., if $b : A \to B$ is a bijection of A onto B, then $\mathcal{S}$ and $b(\mathcal{S})$ have the same intersection pattern. $[X(\mathcal{S})]$ is *forbidden* if $|A| \geq 2$, m is an odd integer in $[3, |A|+1]$ (respectively, $[3, |A|]$) if $|A|$ is even (respectively, odd), $k \in [m-1, \min\{2^{m-1}-1, |A|\}]$, and $[X(\mathcal{S})] \in \mathcal{F}_{mk}(|A|)$. By using a bijection of A onto $[1, |A|]$, we thus deduce immediately from Theorem 2.11 the following result.

Theorem 2.11′ *If A is a nonempty finite set and $\emptyset \neq \mathcal{S} \subseteq 2^A \backslash \{\emptyset\}$, then $\mathcal{S}$ has the odd-intersection property with respect to A if and only if $\mathcal{S}$ does not contain a subset of 2^A with a forbidden intersection pattern.*

In order to state and prove our characterization of the finite subsets of Z^+ that are sets of quadratic nonresidues for infinitely many primes, we first recall that the symmetric difference $A \Delta B$ of sets A and B is defined as $(A \backslash B) \cup (B \backslash A)$. The symmetric difference operation is commutative and associative, hence if $\{A_1, \ldots, A_k\}$ is a finite set of subsets of a fixed set A then the repeated symmetric difference

$$A_1 \Delta A_2 \Delta \cdots \Delta A_k = \Delta_{i=1}^{k} A_i$$

is unambiguously defined. We also note that

$$\Delta_{i=1}^{k} A_i = \{a \in A : |\{A_j : a \in A_j\}| \text{ is odd}\}. \tag{2.2}$$

Theorem 2.12. *If S is a nonempty finite subset of Z^+ which contains no squares, if Π is the set of all prime factors of the elements of S of odd multiplicity, and if $\mathcal{S} = \{\pi_{\text{odd}}(z) : z \in S\}$, then the following statements are equivalent:*

(i) *S is a set of quadratic nonresidues for infinitely many primes;*

(ii) *for each subset T of S of odd cardinality, the product of all the elements of T is not a square;*

(iii) *for each subset $\mathcal{T}$ of $\mathcal{S}$ of odd cardinality, $\Delta_{T \in \mathcal{T}} T \neq \emptyset$;*

(iv) *$\mathcal{S}$ does not contain a subset of 2^{Π} with a forbidden intersection pattern.*

Proof. The equivalence of (i) and (iv) is an immediate consequence of Lemma 1.1 and Theorem 2.11′ and the equivalence of (i) and (ii) follows from [5, Corollary III.A]. In order to see that (i) and (iii) are equivalent, we consider the subset of Z^+ defined by

$$S' = \left\{ \prod_{p \in T} p : T \in \mathcal{S} \right\}.$$

and observe that the elements of S and S' have the same set Π of prime factors of odd multiplicity, that $\mathcal{S} = \{\pi_{\text{odd}}(z) : z \in S'\}$ and that S is a set of quadratic nonresidues for infinitely many primes if and only if S' is also such a set. We may hence suppose without loss of generality that every element of S is square-free, i.e., no element of S has a perfect square as a nontrivial factor. It hence follows that if T is a nonempty subset of S and $\mathcal{T} = \{\pi_{\text{odd}}(z) : z \in T\}$ then $|T| = |\mathcal{T}|$ and the multiplicity of each prime factor p in the product of all the elements of T is $|\{U \in \mathcal{T} : p \in U\}|$. The equivalence of (i) and (iii) now follows from the fact that the map $T \to \mathcal{T}$ is a bijection of 2^S onto $2^{\mathcal{S}}$, equation (2.2), and the equivalence of (i) and (ii).

QED

Replacing a fixed nonempty finite set by a set of primes of the same cardinality and arguing as in the proof of Theorem 2.12, we deduce as our second solution of the basic problem the following internal characterization of the odd-intersection property:

Theorem 2.13. *If A is a nonempty finite set and $\emptyset \neq \mathcal{S} \subseteq 2^A \setminus \{\emptyset\}$, then $\mathcal{S}$ has the odd-intersection property with respect to A if and only if for each subset $\mathcal{T}$ of $\mathcal{S}$ of odd cardinality, $\triangle_{T \in \mathcal{T}} T \neq \emptyset$.*

Remark. If $\mathcal{S}$ is a subset of $2^{[1,n]} \setminus \{\emptyset\}$ of odd cardinality m, then $\triangle_{S \in \mathcal{S}} S = \emptyset$ if and only if the column space of $I(\mathcal{S})$ is contained in $\mathcal{Y}_{m-1}$. This observation can be used to give a direct proof of Theorem 2.13, thereby obviating Corollary III.A of [5] in the argument. Arrangement of the reasoning as we have done makes the proof a bit more economical and it also highlights the close connection between the combinatorics and the number theory.

We next address the question of extending Theorem 2.12 to arbitrary finite sets of nonzero integers. Toward that end let $\pi_{\text{odd}}(z)$ for a negative integer z denote the set of all prime factors of $-z$ of odd multiplicity; if S is a set of integers, then S^+ (respectively, S^-) denotes the set of positive (respectively, negative) elements of S. Employment of the ideas in [14, section 2] and a straight-forward modification of the proof of Theorem 2.12 establishes the following result, the details of which we leave to the interested reader:

Theorem 2.14. *If S is a nonempty finite set of nonzero integers which contains no squares, if Π is the set of all prime factors of the elements of S of odd multiplicity, if $\mathcal{S} = \{\pi_{\text{odd}}(z) : z \in S\}$, and if $\mathcal{S}^{\pm} = \{\pi_{\text{odd}}(z) : z \in S^{\pm}\}$, then the following statements are equivalent:*

(i) *S is a set of quadratic nonresidues for infinitely many primes;*

(ii) *for each subset $\mathcal{T}$ of $\mathcal{S}$ of odd cardinality, the product of all the elements of $\mathcal{T}$ is not a square;*

(iii) *either $\emptyset \notin \mathcal{S}$ and $\mathcal{S}$ satisfies condition (iii) (equivalently, condition (iv)) of Theorem 2.12 or $\mathcal{S}^+ \cap \mathcal{S}^- = \emptyset$ and for each subset $\mathcal{T}$ of $\mathcal{S}$ of odd cardinality, either $|\mathcal{T} \cap \mathcal{S}^-|$ is odd or $\triangle_{T \in \mathcal{T}} T \neq \emptyset$;*

(iv) *for each subset $\mathcal{T}$ of $\mathcal{S}^+ \cup \{\{-1\} \cup W : W \in \mathcal{S}^-\}$ of odd cardinality,*

$$\triangle_{T \in \mathcal{T}} T \neq \emptyset;$$

(v) *$\mathcal{S}^+ \cup \{\{-1\} \cup W : W \in \mathcal{S}^-\}$ does not contain a subset of $2^{\{-1\} \cup \Pi}$ with a forbidden intersection pattern.*

Corollary 2.15. *Every nonempty finite set of negative integers is a set of quadratic nonresidues for infinitely many primes.*

Remarks.(1) Let S be nonempty subset of nonzero integers which is *not* necessarily finite, and suppose S contains no squares. If $\mathcal{S} = \{\pi_{\text{odd}}(z) : z \in S\}$ is finite then statements (i)–(iv) of Theorem 2.14 are still equivalent.

(2) We thank the referee of [15] for pointing out to us the equivalence of statements (iii) and (iv) of Theorem 2.14.

(3) Let $n \geq 2$ be a fixed integer, and let m be an odd integer in $[3, n+1]$ (respectively, $[3, n]$) if n is even (respectively, odd). Recall that $\mathcal{O}_m(n)$ denotes the set of all obstructions in $2^{[1,n]}\backslash\{\emptyset\}$ of cardinality m, and let $OIP(n)$ denote the set of all nonempty subsets of $2^{[1,n]}\backslash\{\emptyset\}$ with the odd-intersection property. In light of our work here, it is of interest to consider the following two counting problems:

What is the cardinality of $\mathcal{O}_m(n)$?
What is the cardinality of $OIP(n)$?

We have obtained an exact and computationally efficient formula for the cardinality of $\mathcal{O}_m(n)$ [16], and V. Scharaschkin [11] has recently found a very nice explicit formula for $OIP(n)$. In particular, the cardinality of $OIP(n)$ has an interpretation that is of some interest for number theory that we will now point out.

Declare a nonempty subset of Z^+ to be *completely square-free* if it does not contain 1 and all of its elements are square-free, i.e., no element has a perfect square as a nontrivial factor. If S is a nonempty, finite, completely square-free subset of Z^+, Π is the set of all prime factors of the elements of S, $\pi(z)$ is the set of prime factors of $z \in S$, and if $\mathcal{S} = \{\pi(z) : z \in S\}$, then S is uniquely determined by $\mathcal{S}$ and vis-versa, S and $\mathcal{S}$ have the same cardinality, and S is a set of quadratic nonresidues for infinitely many primes if and only if $\mathcal{S}$ has the odd-intersection property with respect to Π. On the other hand, if Π is a given nonempty finite set of primes and $\emptyset \neq \mathcal{S} \subseteq 2^{\Pi}\backslash\{\emptyset\}$, we say that

$$\left\{ \prod_{p \in S} p : S \in \mathcal{S} \right\}$$

is a completely square-free set *determined by* Π. Consequently, if Π is a nonempty finite set of primes of cardinality n, then the cardinality of $OIP(n)$ counts the number of completely square-free sets determined by Π that are sets of quadratic nonresidues for infinitely many primes.

3 On the density of primes with a fixed finite set of quadratic residues or nonresidues.

If P denotes the set of all prime numbers and $\Pi \subseteq P$, then the *density of* Π (in P) is defined to be

$$\lim_{x \to +\infty} \frac{|\{p \in \Pi : p \leq x\}|}{|\{p \in P : p \leq x\}|}$$

provided this limit exists. In light of [14, Theorem 2.3] and the results of this paper, it is of interest to consider for a fixed finite subset S of nonzero integers the density of the set of primes p such that S is a set of quadratic residues of p and the density of the set of primes p such that S is a set of quadratic nonresidues of p. We offer two results which, in the spirit of our work here, calculate these densities in terms of certain combinatorial parameters associated with the prime factors of the elements of S of odd multiplicity.

In what follows, p will always denote a generic prime and if z is an integer, $(z \,|\, p)$ will denote the value of the Legendre symbol of p at z. We also recall that if $n \in Z^+$ then $v : 2^{[1,n]} \to F^n$ denotes the bijection defined in the paragraph penultimate to Lemma 2.2, and $V : 2^{2^{[1,n]}} \to 2^{F^n}$ denotes the bijection induced by v, i.e., if $\mathcal{S} \subseteq 2^{[1,n]}$, then $V(\mathcal{S}) = \{v_S : S \in \mathcal{S}\}$.

The proof of the theorems in this section requires two lemmas; the first is an immediate consequence of [4, Theorem 2] and the second is a simple result in enumerative combinatorics.

Lemma 3.1 *If Π is a nonempty finite set of primes, S is either Π or $\{-1\} \cup \Pi$, and $\varepsilon : S \to \{-1, 1\}$ is a choice of signs for the elements of S, then $2^{-|S|}$ is the density of the set $\{p : (z \,|\, p) = \varepsilon(z), \forall z \in S\}$.*

Lemma 3.2 *If A is a nonempty finite set, $n = |A|$, $\mathcal{S}$ and $\mathcal{T}$ are disjoint subsets of 2^A, and d is the dimension of the linear span of $V(\mathcal{S} \cup \mathcal{T})$ in F^n, then the cardinality of the set*

$$\mathcal{P} = \{N \subseteq A : |N \cap S| \text{ is even}, \forall S \in \mathcal{S},\ |N \cap T| \text{ is odd}, \forall T \in \mathcal{T}\}$$

is either 0 or 2^{n-d}.

Proof. We may with no loss of generality take $A = [1, n]$. There is a bijection of the set of all solutions in F^n of the system of linear equations

$$\sum_1^n v_S(i) x_i = 0,\ S \in \mathcal{S},\ \sum_1^n v_T(i) x_i = 1,\ T \in \mathcal{T}$$

onto $\mathcal{P}$ which is defined by

$$(x_1, \ldots, x_n) \leftrightarrow \{i : x_i = 1\}.$$

If this system of equations has no solution then $|\mathcal{P}| = 0$. Otherwise, if $\sigma : F^n \to F^m$, $m = |S \cup T|$, is the linear transformation whose representing matrix is the coefficient matrix of the system, then the set of all solutions of this system has the same cardinality as the kernel of σ. But d is the rank of σ, and so the kernel of σ has dimension $n - d$. Thus the kernel of σ, and hence $\mathcal{P}$, has cardinality 2^{n-d}. QED

In the statement of the following theorem, we use the notation introduced in the paragraph penultimate to Theorem 2.14.

Theorem 3.3 *If S is a nonempty, finite subset of $Z\backslash\{0\}$, $T = S\backslash\{n^2 : n \in Z^+\}$, Π is the set of all prime factors of the elements of T of odd multiplicity, $\mathcal{T} = \{\pi_{\text{odd}}(z) : z \in T\}$, $\mathcal{T}^{\pm} = \{\pi_{\text{odd}}(z) : z \in T^{\pm}\}$,*

$$\mathcal{P}_{eo} = \{N \subseteq \Pi : \ |N \cap U| \text{ is even}, \forall U \in \mathcal{T}^+, \ |N \cap W| \text{ is odd}, \forall W \in \mathcal{T}^-\},$$

d is the dimension of the linear span of $V(\mathcal{T})$ in $F^{|\Pi|}$, and

$$d_+ = \text{ density of } \{p : (z \,|\, p) = 1, \ \forall z \in S\},$$

then

$$d_+ = \begin{cases} 2^{-d}, & \text{if either } \mathcal{T}^- = \emptyset \text{ or } \emptyset \notin \mathcal{T}^- \neq \emptyset \text{ and } \mathcal{P}_{eo} \neq \emptyset, \\ 2^{-(1+d)}, & \text{if either } \emptyset \in \mathcal{T}^- \text{ or } \emptyset \notin \mathcal{T}^- \neq \emptyset \text{ and } \mathcal{P}_{eo} = \emptyset. \end{cases}$$

Proof. Set $n = |\Pi|$, $Q = \{p : (z \,|\, p) = 1, \ \forall z \in S\}$, and let $\mathcal{P}_e = \{N \subseteq \Pi : \ |N \cap U|$ is even, $\forall U \in T\}$. If $p \in Q$ then

$$1 = (z \,|\, p) = \prod_{q \in \pi_{\text{odd}}(z)} (q \,|\, p), \ \forall z \in S^+ \text{ and}$$

$$1 = (-1 \,|\, p) \prod_{q \in \pi_{\text{odd}}(z)} (q \,|\, p), \ \forall z \in S^-.$$

If $(-1 \mid p) = 1$, then

$$1 = \prod_{q \in \pi_{\text{odd}}(z)} (q \mid p), \ \forall z \in S,$$

and so if we set

$$N_\Pi(p) = \{q \in \Pi : \ (q \,|\, p) = -1\},$$

then

$$N_\Pi(p) \in \mathcal{P}_e. \tag{3.1}$$

If $(-1\,|\,p) = -1$, then

$$1 = \prod_{q \in \pi_{\text{odd}}(z)} (q\,|\,p),\ \forall z \in S^+ \text{ and}$$

$$-1 = \prod_{q \in \pi_{\text{odd}}(z)} (q\,|\,p),\ \forall z \in S^-\backslash\{-n^2 :\ n \in Z^+\},$$

hence

$|N_\Pi(p) \cap U|$ is even, $\forall\, U \in \mathcal{T}^+$ and $|N_\Pi(p) \cap W|$ is odd, $\forall\, W \in \mathcal{T}^-\backslash\{\emptyset\}$.

If $\emptyset \in \mathcal{T}^-$, then $(-1|p) = 1$, and so (3.1) is also true in this instance.

Suppose now that $\mathcal{T}^- = \emptyset$, i.e., $S \subseteq Z^+$. If $N \in \mathcal{P}_e$ then $\{p : N_\Pi(p) = N\} \subseteq Q$, hence we may write Q as the pairwise disjoint union

$$\bigcup_{N \in \mathcal{P}_e} \{p : N_\Pi(p) = N\}.$$

As a consequence of Lemma 3.1, each set of this union has density 2^{-n}, hence

$$d_+ = \text{ density of } Q = |\mathcal{P}_e| \cdot 2^{-n}. \tag{3.2}$$

If $\emptyset \in \mathcal{T}^-$ and $N \in \mathcal{P}_e$, then $\{p : (-1|p) = 1,\ N_\Pi(p) = N\} \subseteq Q$, hence in this case, Q is the pairwise disjoint union

$$\bigcup_{N \in \mathcal{P}_e} \{p : (-1|p) = 1,\ N_\Pi(p) = N\}.$$

Another application of Lemma 3.1 shows that each set of this union has density $2^{-(1+n)}$, and so

$$d_+ = |\mathcal{P}_e| \cdot 2^{-(1+n)}. \tag{3.3}$$

Finally, if $\emptyset \notin \mathcal{T}^- \neq \emptyset$ and $N \in \mathcal{P}_e$ (respectively, $N \in \mathcal{P}_{eo}$), then $\{p : (-1|p) = 1,\ N_\Pi(p) = N\}$ (respectively, $\{p :\ (-1|p) = -1,\ N_\Pi(p) = N\}$) is contained in Q. Hence Q is now the pairwise disjoint union

$$\left(\bigcup_{N \in \mathcal{P}_e} \{p : (-1|p) = 1,\ N_\Pi(p) = N\}\right)$$

$$\bigcup\left(\bigcup_{N \in \mathcal{P}_{eo}} \{p : (-1|p) = -1,\ N_\Pi(p) = N\}\right)$$

and a third invocation of Lemma 3.1 yields

$$d_+ = (|\mathcal{P}_e| + |\mathcal{P}_{eo}|) \cdot 2^{-(1+n)}. \tag{3.4}$$

When we now deduce from Lemma 3.2 that $|P_e| = 2^{n-d}$ and $|\mathcal{P}_{eo}|$ is either 0 or 2^{n-d}, the conclusion of Theorem 3.3 then follows from (3.2), (3.3), and (3.4). QED

A similar line of reasoning can be followed to establish

Theorem 3.4 *Let S, Π, $\mathcal{T}$, $\mathcal{T}^{\pm}$, and d be defined as in the statement of Theorem 3.3, and suppose S contains no squares. If*

$$\mathcal{P}_o = \{N \subseteq \Pi : |N \cap U| \text{ is odd}, \forall\, U \in \mathcal{T}\},$$
$$\mathcal{P}_{oe} = \{N \subseteq \Pi : |N \cap U| \text{ is odd}, \forall\, U \in \mathcal{T}^+,\ |N \cap W| \text{ is even}, \forall\, W \in \mathcal{T}^-\},$$

and

$$d_- = \text{ density of } \{p : (z\,|\,p) = -1,\ \forall\, z \in S\},$$

then

$$d_- = \begin{cases} 2^{-d}, & \text{if either } \mathcal{T}^- = \emptyset \text{ and } \mathcal{P}_o \neq \emptyset \text{ or } \emptyset \notin \mathcal{T}^- \neq \emptyset \text{ and} \\ & \mathcal{P}_o \neq \emptyset \neq \mathcal{P}_{oe}, \\ 2^{-(1+d)}, & \text{if either } \emptyset \in \mathcal{T}^- \text{ and } \mathcal{P}_{oe} \neq \emptyset \text{ or } \emptyset \notin \mathcal{T}^- \neq \emptyset \text{ and either} \\ & \mathcal{P}_o \neq \emptyset = \mathcal{P}_{oe} \text{ or } \mathcal{P}_o = \emptyset \neq \mathcal{P}_{oe}, \\ 0, & \text{if } \mathcal{P}_o = \emptyset = \mathcal{P}_{oe}. \end{cases}$$

In light of Theorems 3.3 and 3.4, it is of interest to decide when $\mathcal{P}_{eo}$ (respectively, $\mathcal{P}_{oe}$) is nonempty. The following proposition, a consequence of Theorem 2.14 (see [15, Lemma 2.3 and its proof]), provides combinatorial criteria for doing that.

Proposition 3.5 *The following statements are equivalent:*

(i) $\mathcal{P}_{eo}$ *(respectively,* $\mathcal{P}_{oe}$*) is nonempty;*

(ii) $\mathcal{T}^+ \cap \mathcal{T}^- = \emptyset$ *and for each subset* $\mathcal{U}$ *of* $\mathcal{T}^+ \cup \mathcal{T}^- \cup \{\emptyset\}$ *of odd cardinality, either* $|\mathcal{U} \cap (\mathcal{T}^+ \cup \{\emptyset\})|$ *(respectively,* $|\mathcal{U} \cap (\mathcal{T}^- \cup \{\emptyset\})|$*) is odd or* $\triangle_{U \in \mathcal{U}} U \neq \emptyset$;

(iii) *For each subset* $\mathcal{U}$ *of* $(\mathcal{T}^- \setminus \{\emptyset\}) \cup \{\{-1\} \cup X : X \in \mathcal{T}^+ \cup \{\emptyset\}\}$ *(respectively,* $\mathcal{T}^+ \cup \{\{-1\} \cup X : X \in \mathcal{T}^- \cup \{\emptyset\}\}$*) of odd cardinality,*

$$\triangle_{U \in \mathcal{U}} U \neq \emptyset;$$

(iv) $(\mathcal{T}^- \setminus \{\emptyset\}) \cup \{\{-1\} \cup X : X \in \mathcal{T}^+ \cup \{\emptyset\}\}$ (*respectively,* $\mathcal{T}^+ \cup \{\{-1\} \cup X : X \in \mathcal{T}^- \cup \{\emptyset\}\}$) *does not contain a subset of* $2^{\{-1\} \cup \Pi}$ *with a forbidden intersection pattern.*

Remarks. (1) If follows immediately from Theorem 3.4 that if S is a nonempty, finite subset of $Z \setminus \{0\}$ then the density of $\{p : (z|p) = -1, \forall z \in S\}$ is 0 if and only if $\{p : (z \mid p) = -1, \forall z \in S\}$ is empty.

(2) Suppose that S is a nonempty, finite set of *negative* integers. Then $\mathcal{T}^+ = \emptyset \neq \mathcal{P}_{oe}$, $\emptyset \neq \mathcal{T}^- = \mathcal{T}$, and so it follows from Theorem 3.4 that the density of $\{p : (z \mid p) = -1, \forall z \in S\}$ is 2^{-d} if $\mathcal{P}_o \neq \emptyset$ and $S \cap \{-n^2 : n \in Z^+\} = \emptyset$, and $2^{-(1+d)}$ otherwise. This example illustrates clearly how the combinatorial structure of the prime factorizations of the elements of S determines the size of the set of primes which have S as a set of quadratic nonresidues.

(3) Let S be a nonempty, finite subset of Z^+, let $\sigma = |S \cap \{n^2 : n \in Z^+\}|$, and let r be a non-negative integer. In [15] we characterize when S contains precisely $r + \sigma$ quadratic residues of p, for infinitely many primes p, by means of a purely combinatorial condition on the set of prime factors of the elements of S of odd multiplicity. This result simultaneously generalizes Theorem 2.12 above and [14, Theorem 2.3]. Moreover, [15] also contains a calculation of the density of the set

$$\{p : S \text{ contains exactly } r + \sigma \text{ quadratic residues of } p\}$$

which, for the special case of finite subsets of Z^+, simultaneously generalizes Theorems 3.3 and 3.4. However, the results of [15] do not obviate the results of this paper. Indeed, the proofs of the former make essential use of Theorem 2.14 and Lemmas 3.1 and 3.2 of the latter.

References

[1] B. Berndt, Classical theorems on quadratic residues, Enseignement Math., 22 (1976) 261–304.

[2] D. Buell and R. Hudson, On runs of consecutive quadratic residues and quadratic nonresidues, BIT, 24 (1984) 243–247.

[3] P. G. L. Dirichlet, Recherches sur diverses applications de l'analyse infinitésimale à la théorie des nombres, J. Reine Angew. Math., 19 (1839) 324–369.

[4] M. Filaseta and D. Richman, Sets which contain a quadratic residue modulo p for almost all p, Math. J. Okayama Univ., 39 (1989) 1–8.

[5] M. Fried, Arithmetical properties of value sets of polynomials, Acta Arith., 15 (1969) 91–115.

[6] E. Hecke, Vorlesungen über die Theorie der Algebraischen Zahlen (Leipzig, 1923).

[7] D. Hilbert, Die Theorie der algebraischen Zahlkörper, Jahresbericht der Deutschen Mathematiker-Vereinigung, 4 (1897) 175-546.

[8] R. Hudson, On the first occurrence of certain patterns of quadratic residues and nonresidues, Israel J. Math., 44 (1983) 23–32.

[9] F. Lemmermeyer, Reciprocity Laws, (Springer-Verlag, Berlin, 2000).

[10] M. Monzingo, On the distribution of consecutive triples of quadratic residues and quadratic nonresidues and related topics, Fibonacci Quart., 23 (1985) 133–138.

[11] V. Scharaschkin, The odd and even intersection properties, preprint.

[12] A. Schinzel, On power residues and exponential congruences, Acta Arith., 27 (1975) 397–420.

[13] A. Schinzel and M. Skalba, On power residues, Acta Arith., 108 (2003) 77–94.

[14] S. Wright, Patterns of quadratic residues and nonresidues for infinitely many primes, J. Number Theory,123 (2007) 120–132.

[15] S. Wright, Quadratic residues and the combinatorics of sign multiplication, J. Number Theory, 128 (2008) 918–925.

[16] S. Wright, Some enumerative combinatorics arising from a problem on quadratic nonresidues, Australasian J. Combinatorics, 44 (2009) 301–315.