AUSTRALASIAN JOURNAL OF COMBINATORICS
Volume **44** (2009), Pages 301–315

Some enumerative combinatorics arising from a problem on quadratic nonresidues

Steve Wright

Department of Mathematics and Statistics
Oakland University
Rochester, MI 48309-4485
U.S.A.
wright@oakland.edu

Abstract

If A is a finite set of cardinality $n \geq 1$, 2^A is the set of all subsets of A, and $\mathcal{S}$ is a nonempty subset of 2^A, we say that $\mathcal{S}$ has the *odd-intersection property* if there exists a subset N of A such that the cardinality of $N \cap S$ is odd for each $S \in \mathcal{S}$. Let $OIP(n)$ denote the set of all subsets of 2^A with the odd-intersection property. A nonempty set $\mathcal{S}$ of nonempty subsets of A is an *obstruction* (to the odd-intersection property) if $\mathcal{S}$ does not have the odd-intersection property, but all nonempty proper subsets of $\mathcal{S}$ do have it. Let $\mathcal{O}(n)$ denote the set of all obstructions that are contained in 2^A. This paper initiates a study of the cardinality of $\mathcal{O}(n)$ and $OIP(n)$. Interest in this problem arose from previous work of the author on a combinatorial characterization of the finite subsets S of the positive integers with the following property: for infinitely many prime numbers p, S is a set of quadratic nonresidues of p.

1 Introduction

If n is a positive integer and if $[1, n]$ denotes the n-set $\{1, \ldots, n\}$, $2^{[1,n]}$ denotes the set of all subsets of $[1, n]$, and $\emptyset$ denotes the empty set, then a nonempty subset $\mathcal{S}$ of $2^{[1,n]}$ is said to have the *odd-intersection property relative to* $[1, n]$ if there exists a subset N of $[1, n]$ such that the cardinality of $N \cap S$ is odd for each element S of $\mathcal{S}$. We let $OIP(n)$ denote the set of all subsets of $2^{[1,n]}$ with the odd-intersection property. A nonempty subset $\mathcal{S}$ of $2^{[1,n]} \backslash \{\emptyset\}$ is said to be on *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 because of the following simple fact: a nonempty subset of $2^{[1,n]} \backslash \{\emptyset\}$ has the odd-intersection property if and only if it does not contain an obstruction. Let $\mathcal{O}(n)$ denote the set of all obstructions that are contained in $2^{[1,n]}$. The purpose of this

paper is to investigate the following two counting problems:

$$\text{What is the cardinality of } \mathcal{O}(n)? \tag{1.1}$$

$$\text{What is the cardinality of } OIP(n)? \tag{1.2}$$

Of course, there is nothing sacred here about the n-set $[1, n]$. One can replace it by any set of cardinality n and formulate the appropriate notions of odd-intersection property and obstructions relative to that set.

Our interest in problems (1.1) and (1.2) arose from the work of [6, 7] concerning the following problem in elementary number theory. If Z^+ denotes the set of positive integers and $p \in Z^+$ is prime, an integer z is a *quadratic nonresidue of* p if the modular congruence $x^2 \equiv z \mod p$ does not have an integer solution x. In [7], motivated by the work of Buell and Hudson [1], Filaseta and Richman [2], Hudson [3], and Monzingo [4], we characterized the nonempty finite subsets S of Z^+ such that for infinitely many primes p, every element of S is a quadratic nonresidue of p. Our characterization was formulated combinatorially in terms of the odd-intersection property in the following way: if $z \in S$, if $\pi_{\text{odd}}(z)$ denotes the set of prime factors of z of odd multiplicity, and if Π denotes 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 S contains no squares and the set $\{\pi_{\text{odd}}(z) : z \in S\}$ has the odd-intersection property relative to Π ([6, Lemma 2.5]). Given a nonempty finite set Π of primes, it hence follows that solutions to problems (1.1) and (1.2) give information on the number of subsets of Z^+ which can be formed from products of the elements of Π that are sets of quadratic nonresidues for infinitely many primes (see the remark at the end of Section 3 for a more precise and detailed discussion of this).

We now briefly describe the contents of this paper. Section 2 presents two results that constitute the principal tools that we use to study problems (1.1) and (1.2): the atomic decomposition of a family of sets and a result from [7] that determines the structure of the obstructions that are contained in $2^{[1,n]}$. The principal results of this paper are Theorems 3.5 and 3.8 in Section 3, which give exact formulas for the cardinalities of $\mathcal{O}(n)$ and $OIP(n)$, respectively. We also perform some calculations in Section 3 which explicitly compute the cardinalities of $\mathcal{O}(n)$ and $OIP(n)$ for various (small) values of n.

2 Atomic decomposition and structure of obstructions

In all of what follows, the following notation will be employed: if m and n are integers with $2 \leq m \leq n$, then $[m, n]$ will denote the set of all elements of the n-set $[1, n]$ that exceed $m - 1$ and if A is a set, then $|A|$ will denote the cardinality of A and 2^A will denote the set of all subsets of A.

Now, let $F = \{0, 1\}$ denote the Galois field $Z/2Z$ of order 2, and let F^n denote the vector space of dimension $n \in Z^+$ over F. We will use linear algebra in F^n to study subsets of $2^{[1,n]}$ by means of the following familiar device. If $S \subseteq [1, n]$, then 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 and if $\mathcal{S} \subseteq 2^{[1,n]}$, then we will let $V(\mathcal{S})$ denote the set $\{v_S : S \in \mathcal{S}\}$.

If $\emptyset \neq V = \{v_1, \ldots, v_m\} \subseteq F^n \backslash \{0\}$, then the *incidence matrix of* V is defined to be the $m \times n$ matrix over F whose (i,j)-entry is $v_i(j)$. If $\emptyset \neq \mathcal{S} \subseteq 2^{[1,n]} \backslash \{\emptyset\}$, then the *incidence matrix* $I(\mathcal{S})$ *of* $\mathcal{S}$ is defined to be the incidence matrix of $V(\mathcal{S})$, and we define the *column set* $C(\mathcal{S})$ of $\mathcal{S}$ to be the set of all nonzero columns of $I(\mathcal{S})$. We note that $C(\mathcal{S}) \subseteq F^m \backslash \{0\}$, where $m = |\mathcal{S}|$.

The principle tool that we will use to investigate the cardinality of $\mathcal{O}(n)$ and $OIP(n)$ is the atomic decomposition of a class of sets. This decomposition exists for any subset of 2^A, where A is an arbitrary set, but we will describe it only for nonempty subsets of $2^{[1,n]} \backslash \{\emptyset\}$ in terms of their incidence matrices, since that will be its most convenient form for the work to be done here.

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 for each $i \in [1,m]$, there exists $c \in C$ such that $c(i) = 1$ 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 $\{S_1, \ldots, S_m\}$ 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, and we will call this equivalence class the *intersection pattern of* 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 the intersection pattern of X, and this definition clearly does not depend on how X is formed from an ordering of the elements of $C(\mathcal{S})$.

Our next task is to describe the structure of an obstruction in $2^{[1,n]}$. This will require some preliminary definitions and companion notation. To that end, we first associate to each odd integer $m \geq 3$ the subspace $\mathcal{Y}_{m-1}$ of F^m consisting of all vectors with an odd number of 0 coordinates. The dimension of $\mathcal{Y}_{m-1}$ is $m-1$. Now 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 then set

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

If X is a matrix of size $m \times k$ whose column set is an element of $\mathcal{C}_{mk}(n)$, we will call the intersection pattern of X *forbidden* and we will denote by $\mathcal{F}_{mk}(n)$ the set of all forbidden intersection patterns which arise in this way from elements of $\mathcal{C}_{mk}(n)$.

There is a parametrization of the elements of $\mathcal{F}_{mk}(n)$ that will prove useful in the enumerative combinatorics that we study in section 3. 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 $U \subseteq F^m$. If we now observe that $\mathcal{C}_{mk}(n)$ is invariant under any permutation of the coordinates of F^m then the following lemma is evident from the construction of forbidden intersection patterns given above:

Lemma 2.1 *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 $k \in [m-1,\ \min\{2^{m-1}-1, n\}]$, 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*

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

We can now state the following result, which describes precisely the structure of the obstructions contained in $2^{[1,n]}$.

Theorem 2.2 ([7, Proposition 2.7 and Theorem 2.11]). *Let $n \geq 2$ be an integer. If $\emptyset \neq \mathcal{O} \subseteq 2^{[1,n]}\backslash\{\emptyset\}$, then $\mathcal{O}$ is an obstruction if and only if the cardinality m of $\mathcal{O}$ is an odd integer in $[3, n+1]$ (respectively, $[3, n]$) if n is even (respectively, odd) and there exists $k \in [m-1,\ \min\{2^{m-1}-1, n\}]$ such that the intersection pattern of $\mathcal{O}$ is in $\mathcal{F}_{mk}(n)$.*

3 The cardinality of $\mathcal{O}(n)$ and $OIP(n)$

Let $n \geq 2$ be an integer and let m be an odd integer in $[3, n+1]$ (respectively, $[3, n]$) if n is even (respectively, odd). Let $\mathcal{O}_m(n)$ denote the set of all obstructions $\mathcal{O} \subseteq 2^{[1,n]}$ such that $|\mathcal{O}| = m$. It follows from Theorem 2.2 that $\mathcal{O}(n)$ is the pairwise disjoint union of the $\mathcal{O}_m(n)$'s, and so in order to calculate the cardinality of $\mathcal{O}(n)$, it suffices to calculate the cardinality of $\mathcal{O}_m(n)$ for each relevant value of m.

The atomic decomposition will be our primary tool for the investigation of the cardinality of $\mathcal{O}_m(n)$; we will need to supplement it by a lemma which indicates how a subset of $2^{[1,n]}$ is uniquely determined by its atomic decomposition. For that, let $\emptyset \neq \mathcal{S} \subseteq 2^{[1,n]} \backslash \{\emptyset\}$, with $m = |\mathcal{S}|$ and with column set $C(\mathcal{S})$. If $i \in [1, m]$, the *i-th incidence set* $I_i(\mathcal{S})$ *of* $\mathcal{S}$ is defined by

$$I_i(\mathcal{S}) = \{c \in C(\mathcal{S}) : \ c(i) = 1\}.$$

The following straightforward lemma provides the required uniqueness criterion:

Lemma 3.1 *If $\mathcal{S}_\ell$ is a nonempty subset of $2^{[1,n]} \backslash \{\emptyset\}$ with column set C_ℓ, set of atoms A_ℓ, attachment map $b_\ell : \ C_\ell \to A_\ell$, and incidence sets $\{I_{\ell i} : \ i \in [1, |\mathcal{S}_\ell|]\}$, $\ell = 1, 2$, then $\mathcal{S}_1 = \mathcal{S}_2$ if and only if*

(a) $|\mathcal{S}_1| = |\mathcal{S}_2|$,

(b) $A_1 = A_2$, *and*

(c) if $|\mathcal{S}_1| = m = |\mathcal{S}_2|$, *then there exists a permutation* σ *of the coordinates of* F^m *and a permutation* τ *of* $[1, m]$ *such that* $\sigma(C_1) = C_2$ *and*

$$b_1(I_{1i}) = b_2\sigma(I_{1\tau(i)}), \ i \in [1, m],$$

i.e., $\sigma^{-1}b_2^{-1}b_1$ *permutes the incidence sets of* $\mathcal{S}_1$.

Remark. If $\sigma(C_1) = C_2$ as in condition (c) of Lemma 3.1, then $\sigma^{-1}b_2^{-1}b_1$ permutes the incidence sets of $\mathcal{S}_1$ if and only if $\sigma b_1^{-1}b_2$ permutes the incidence sets of $\mathcal{S}_2$.

In order to use Lemma 3.1 to count the elements of $\mathcal{O}_m(n)$, we require some information about the incidence sets of arbitrary 0-1 matrices. Toward that end, we thus consider a fixed matrix $X = (x_{ij})$ with distinct rows and columns, of size $m \times k$, say, each of whose entries is either a 0 or a 1. The *i-th row-incidence set* $I_i(X)$ *of* X is defined as

$$I_i(X) = \{j : \ x_{ij} = 1\}, \ i \in [1, m],$$

and the *j-th column-incidence set* $J_j(X)$ *of* X is defined as

$$J_j(X) = \{i : \ x_{ij} = 1\}, \ j \in [1, k].$$

If $r \in Z^+$, we let Σ_r denote the full symmetric group on r letters, and set

$$S(X) = \{\sigma \in \Sigma_k : \ \sigma \text{ permutes the row-incidence sets of } X\},$$

$$T(X) = \{\tau \in \Sigma_m : \ \tau \text{ permutes the column-incidence sets of } X\}.$$

Lemma 3.2 *$S(X)$ (respectively, $T(X)$) is a subgroup of Σ_k (respectively, Σ_m), and $|S(X)| = |T(X)|$.*

Proof. That $S(X)$ and $T(X)$ are subgroups of the appropriate symmetric group is clear. The easiest way to see that they have the same order is to observe that $\sigma \in \Sigma_k$ (respectively, $\tau \in \Sigma_m$) is in $S(X)$ (respectively, $T(X)$) if and only if the permutation of the columns (respectively, rows) of X induced by σ (respectively, τ) also permutes the rows (respectively, columns) of X, that the resulting permutation of the rows (respectively, columns) of X determines a unique permutation in $T(X)$ (respectively, $S(X)$), and that the resulting map $S(X) \to T(X)$ (respectively, $T(X) \to S(X)$) is injective. QED

We use the row-incidence sets of X to define an equivalence relation $\sim_X$ on Σ_k as follows: if $(\sigma, \tau) \in \Sigma_k \times \Sigma_k$, then $\sigma \sim_X \tau$ if $\sigma^{-1}\tau$ permutes the row-incidence sets of X. The set of equivalence classes of $\sim_X$ in Σ_k is just the set of left cosets of $S(X)$ in Σ_k, hence

$$[\Sigma_k : S(X)] = \text{ the cardinality of the set of equivalence classes of } \sim_X \text{ in } \Sigma_k. \quad (3.1)$$

Suppose X is now a representative from an intersection pattern $\mathcal{I}$ of a nonempty subset of $2^{[1,n]}\backslash\{\emptyset\}$. The cardinality $\pi(X)$ of the set of equivalence classes of $\sim_X$ in Σ_k does not depend on the representative X taken from $\mathcal{I}$; we hence refer to the common value of $\pi(X)$ for $X \in \mathcal{I}$ as the *assembly index of* $\mathcal{I}$.

We now apply the above technology to the set of obstructions in $2^{[1,n]}$. Let m be an odd integer as defined at the beginning of section 3, let $s(m,n) = \min\{2^{m-1} - 1,\ n\}$, and let k be a fixed integer in $[m-1,\ s(m,n)]$. We recall from section 2 that

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

where $\mathcal{Y}_{m-1}$ denotes the subspace of F^m consisting of all vectors with an odd number of 0 coordinates. The symmetric group Σ_m acts on $\mathcal{C}_{mk}$ by permutation of coordinates; if we set

$$o(m,k) = \text{ set of } \Sigma_m\text{-orbits in } \mathcal{C}_{mk}$$

and for each $\sigma \in o(m,k)$ let X_σ denote an $m \times k$ matrix whose column set is a representative of σ, it follows from Lemma 2.1 that

$$\{[X_\sigma] : \sigma \in o(m,k)\}$$

is the set of all forbidden intersection patterns of size $m \times k$. We can now state the following lemma, which follows directly from Theorem 2.2, Lemma 3.1, and the definition of $\sim_{X_\sigma}$:

Lemma 3.3 *If $n, m, k, o(m,k)$, and X_σ for $\sigma \in o(m,k)$ are as defined above, if $\mathcal{A} = \{A_1, \ldots, A_k\}$ is a set of atoms of cardinality k contained in $2^{[1,n]}\backslash\{\emptyset\}$, if π_σ denotes the assembly index of $[X_\sigma]$, if $\{\tau_1, \ldots, \tau_{\pi_\sigma}\}$ is a complete set of representatives for the equivalence classes of $\sim_{X_\sigma}$, and if*

$$S_{is} = \bigcup_{j \in I_i(X_\sigma)} A_{\tau_s(j)},\ i \in [1,m],\ s \in [1,\pi_\sigma],$$

then $\{\{S_{1s}, \ldots, S_{ms}\} : s \in [1, \pi_\sigma]\}$ *is the set of all obstructions contained in* $2^{[1,n]}$ *of cardinality* m*, intersection pattern* $[X_\sigma]$*, and set of atoms* $\mathcal{A}$.

At this point, an example may be instructive. Let $n = 4,\ m = 5,\ k = 4$, and consider the three 0-1 matrices

$$X_1 = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 1 & 1 & 1 \end{pmatrix},\ X_2 = \begin{pmatrix} 0 & 1 & 1 & 1 \\ 1 & 0 & 1 & 0 \\ 1 & 1 & 0 & 0 \\ 1 & 1 & 1 & 0 \\ 1 & 1 & 1 & 1 \end{pmatrix},\ X_3 = \begin{pmatrix} 0 & 1 & 1 & 0 \\ 1 & 0 & 0 & 1 \\ 0 & 1 & 0 & 1 \\ 1 & 1 & 1 & 0 \\ 0 & 1 & 0 & 0 \end{pmatrix}.$$

The column sets of X_1, X_2, and X_3 are all bases of $\mathcal{Y}_4$, and so $[X_1]$, $[X_2]$, and $[X_3]$ are forbidden intersection patterns. We also have that

$$S(X_1) = \Sigma_4,\ S(X_2) = \{\text{identity, } (23)\},\ S(X_3) = \{\text{identity}\}.$$

It hence follows from (3.1) that the assembly indices of $[X_1]$, $[X_2]$, and $[X_3]$ are, respectively, 1, 12, and 24, and so we conclude from Lemma 3.3 that there is a unique obstruction in $2^{[1,4]}$ with intersection pattern $[X_1]$ (namely the obstruction $\{\{1\}, \{2\}, \{3\}, \{4\}, \{1,2,3,4\}\}$), 12 obstructions with intersection pattern $[X_2]$, and 24 obstructions with intersection pattern $[X_3]$.

Letting $\mathcal{A}(n,k)$ denote the set of all subsets $\mathcal{S}$ of $2^{[1,n]}\backslash\{\emptyset\}$ such that $|\mathcal{S}| = k$ and the elements of $\mathcal{S}$ are pairwise disjoint and setting $a(n,k) = |\mathcal{A}(n,k)|$, we deduce the following lemma from Lemma 3.1, (3.1), and Lemma 3.3.

Lemma 3.4 *If* $n, m,\ s(m,n),\ k,\ o(m,k)$*, and* X_σ *for* $\sigma \in o(m,k)$ *are as defined above, then*

$$|\mathcal{O}_m(n)| = \sum_{k=m-1}^{s(m,n)} a(n,k) \sum_{\sigma \in o(m,k)} [\Sigma_k :\ S(X_\sigma)]\,.$$

Determination of $a(n,k)$

We recall that a subset $\mathcal{P}$ of $2^{[1,n]}\backslash\{\emptyset\}$ is a *partition of* $[1,n]$ *with* k *blocks* if the elements of $\mathcal{P}$ are pairwise disjoint, their union is $[1,n]$, and $|\mathcal{P}| = k$. For each $k \in [1,n]$, we let Π_k denote the set of all partitions of $[1,n]$ with k blocks. Observe next that $\mathcal{A}(n,k)$ is the disjoint union of Π_k and the set Π of all subsets $\mathcal{S}$ of $2^{[1,n]}\backslash\{\emptyset\}$ such that $|\mathcal{S}| = k$, the elements of $\mathcal{S}$ are pairwise disjoint, and the complement in $[1,n]$ of the union of the elements of $\mathcal{S}$ is nonempty.

We next define the map $\rho :\ \Pi \to \Pi_{k+1}$ by

$$\rho(\mathcal{S}) = \mathcal{S} \cup \left\{ [1,n] \backslash \left(\bigcup_{S \in \mathcal{S}} S \right) \right\}.$$

This map is clearly surjective, and for each element $\mathcal{P}$ of Π_{k+1}, $\rho^{-1}(\mathcal{P})$ consists of $k+1$ elements of Π. Since inverse images under ρ of distinct elements of Π_{k+1} are pairwise disjoint, it follows that

$$a(n,k) = |\mathcal{A}(n,k)| = |\Pi_k| + (k+1)|\Pi_{k+1}|.$$

But it is well-known that the elements of Π_k are counted by the Stirling numbers $S(n,k)$ of the second kind ([5, p. 33]), hence

$$a(n,k) = S(n,k) + (k+1)S(n,k+1). \tag{3.2}$$

From (3.2) and the recurrence relation $S(0,0) = 1,\ S(n,k) = kS(n-1,k) + S(n-1,\ k-1)$ for $S(n,k)$, we deduce the recurrence relation for $a(n,k)$:

$$a(0,0) = 1,\ a(n,k) = (k+1)a(n-1,k) + a(n-1,\ k-1).$$

We also deduce from the explicit formula for $S(n,k)$ ([5, p.34]) the following explicit formula for $a(n,k)$:

$$a(n,k) = \frac{1}{k!}\left((k+1)^n + \sum_{i=0}^{k} \frac{(-1)^{k+1-i}}{k+1-i}\binom{k}{i} i^{n+1}\right).$$

Evaluation of $\displaystyle\sum_{\sigma\in o(m,k)} [\Sigma :\ S(X_\sigma)]$

We choose a representative $C_\sigma \in \mathcal{C}_{mk}$ from each $\sigma \in o(m,k)$ and let X_σ be a matrix of size $m \times k$ whose column set is C_σ. The isotropy group of C_σ under the action of Σ_m on $\mathcal{C}_{mk}$ is $T(X_\sigma)$, hence

$$|\mathcal{C}_{mk}| = \sum_{\sigma\in o(m,k)} |\sigma| = \sum_{\sigma\in o(m,k)} [\Sigma_m :\ T(X_\sigma)]\,.$$

By virtue of Lemma 3.2,

$$|T(X_\sigma)| = |S(X_\sigma)|,$$

and so from Lagrange's theorem it follows that

$$[\Sigma_m :\ T(X_\sigma)] = \frac{m!}{k!}\,[\Sigma_k :\ S(X_\sigma)]\,.$$

Hence

$$\begin{aligned}\sum_{\sigma\in o(m,k)} [\Sigma_k :\ S(X_\sigma)] &= \frac{k!}{m!}\sum_{\sigma\in o(m,k)} [\Sigma_m :\ T(X_\sigma)] \\ &= \frac{k!}{m!}|\mathcal{C}_{mk}|.\end{aligned} \tag{3.3}$$

Remark. If $\emptyset \neq \mathcal{S} \subseteq 2^{[1,n]}\backslash\{\emptyset\}$, we will say that $\mathcal{S}$ is *nondegenerate* if $\cup_{S\in\mathcal{S}} S = [1,n]$ and we will say that $\mathcal{S}$ is *essential* if the columns of the incidence matrix $I(\mathcal{S})$ of $\mathcal{S}$ are all distinct and linearly independent over F. One can prove ([7, Lemma 2.6]) that if an obstruction $\mathcal{O} \subseteq 2^{[1,n]}$ is nondegenerate and essential then n is even and $|\mathcal{O}| = n+1$. Moreover, if $\mathcal{O}$ is any obstruction then $\mathcal{O}$ is either nondegenerate (respectively, essential) or can be "expanded" (respectively, "reduced") to a nondegenerate (respectively, essential) obstruction by the addition to $I(\mathcal{O})$ of appropriate columns from the column space of $I(\mathcal{O})$ (respectively, by the deletion from $I(\mathcal{O})$ of

appropriate columns). The nondegenerate essential obstructions can hence be regarded as "irreducible" in a certain sense, and they in fact play a key role in the determination of the structure of an arbitrary obstruction ([7, Section 2]).

If n is even, it follows from the preceding calculations that the cardinality of the set of all nondegenerate essential obstructions contained in $2^{[1,n]}$ is

$$a(n,n) \sum_{\sigma \in o(n+1,n)} [\Sigma_n : \ S(X_\sigma)]$$

and so we deduce from (3.3) that this cardinality is

$$\begin{aligned} \frac{1}{n+1}|\mathcal{C}_{n+1,n}| &= \frac{1}{n+1}|\text{ set of all bases of } \mathcal{Y}_n| \\ &= \frac{1}{(n+1)!}\prod_{i=0}^{n-1}(2^n - 2^i). \end{aligned}$$

Thus for $n = 2$, 4, 6, and 8, the number of these obstructions is respectively, 1, 168, 83328, and 14737830051840. This gives some indication of how rapidly the cardinality of the set of all obstructions in $2^{[1,n]}$ increases as n increases.

The next theorem, the principle result of this section, is now an immediate consequence of Lemma 3.4 and the calculations which follow that lemma:

Theorem 3.5 *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 $\mathcal{O}_m(n)$ be the set of all obstructions of cardinality m that are contained in $2^{[1,n]}$. If $s(m,n) = \min\{2^{m-1} - 1, n\}$, then*

$$|\mathcal{O}_m(n)| = \frac{1}{m!}\sum_{k=m-1}^{s(m,n)} b(n,k) \cdot c(m,k),$$

where

$$b(n,k) = (k+1)^n + \sum_{i=0}^{k} \frac{(-1)^{k+1-i}}{k+1-i}\binom{k}{i} i^{n+1},$$

with recurrence relation

$$b(0,0) = 1, \ b(n,k) = (k+1)b(n-1,k) + kb(n-1,k-1),$$

and $c(m,k)$ is the cardinality of the set

$$\left\{C \subseteq F^{m-1}\backslash\{0\} : \ |C| = k \text{ and } C \text{ contains a basis of } F^{m-1}\right\},$$

where

$$F^{m-1} = \text{ the vector space of dimension } m-1 \text{ over } F.$$

We will now illustrate the use of Theorem 3.5 by counting all of the various sets of obstructions in $2^{[1,n]}$ for $n = 2$, 3, 4, and 5.

$n = 2$

$$|\mathcal{O}(2)| = |\mathcal{O}_3(2)| = \frac{1}{3!}b(2,2)\cdot c(3,2) = \frac{1}{3!}\cdot 2\cdot 3 = 1$$

$n = 3$

$$\begin{aligned}|\mathcal{O}(3)| &= |\mathcal{O}_3(3)|\\ &= \frac{1}{3!}b(3,2)\cdot c(3,2) + \frac{1}{3!}b(3,3)\cdot c(3,3)\\ &= \frac{1}{3!}\cdot 12\cdot 3 + \frac{1}{3!}\cdot 6\cdot 1\\ &= 7.\end{aligned}$$

$n = 4$

$$\begin{aligned}|\mathcal{O}(4)| &= |\mathcal{O}_3(4)| + |\mathcal{O}_5(4)|.\\ |\mathcal{O}_3(4)| &= \frac{1}{3!}b(4,2)\cdot c(3,2) + \frac{1}{3!}b(4,3)\cdot c(3,3)\\ &= \frac{1}{3!}\cdot 50\cdot 3 + \frac{1}{3!}\cdot 60\cdot 1\\ &= 35,\\ |\mathcal{O}_5(4)| &= \frac{1}{5!}b(4,4)\cdot c(5,4)\\ &= \frac{1}{5!}\cdot 24\cdot 840\\ &= 168.\\ |\mathcal{O}(4)| &= 35 + 168 = 203.\end{aligned}$$

$\boldsymbol{n = 5}$

$$\begin{aligned}
|\mathcal{O}(5)| &= |\mathcal{O}_3(5)| + |\mathcal{O}_5(5)|.\\
|\mathcal{O}_3(5)| &= \frac{1}{3!}b(5,2)\cdot c(3,2) + \frac{1}{3!}b(5,3)\cdot c(3,3)\\
&= \frac{1}{3!}\cdot 180\cdot 3 + \frac{1}{3!}\cdot 390\cdot 1\\
&= 155.\\
|\mathcal{O}_5(5)| &= \frac{1}{5!}b(5,4)\cdot c(5,4) + \frac{1}{5!}b(5,5)\cdot c(5,5)\\
&= \frac{1}{5!}\cdot 360\cdot 840 + \frac{1}{5!}\cdot 120\cdot c(5,5)\\
&= 2520 + c(5,5).
\end{aligned}$$

Our task now is to count the elements of $\mathcal{C}_{55}$, and we will do this by means of the simple "disjointify and fibrate" technique that was used in the determination of $a(n,k)$. Letting $\mathcal{B}$ denote the set of all bases of F^4, which has cardinality 840, we begin by noting that every 5-element subset of $F^4\backslash\{0\}$ which contains a basis is of the form

$$b \cup \left\{\sum_{v\in S} v\right\},$$

where $b \in \mathcal{B},\ S \subseteq b$, and $|S| \geq 2$. For k = 1,2, or 3, define

$$\mathcal{C}(k) = \left\{ b \cup \left\{\sum_{v\in S} v\right\} :\ b\in\mathcal{B},\ S\subseteq b,\ |S| = k+1 \right\}.$$

The required disjointification is provided by the following lemma:

Lemma 3.6 $\mathcal{C}(1)$, $\mathcal{C}(2)$, *and* $\mathcal{C}(3)$ *are pairwise disjoint with union* $\mathcal{C}_{55}$.

Proof. We have already noted that $\mathcal{C}_{55}$ is the union of $\mathcal{C}(1)$, $\mathcal{C}(2)$, and $\mathcal{C}(3)$, so we need only verify disjointness.

Let

$$b_i = \{b_{i1},\ b_{i2},\ b_{i3},\ b_{i4}\} \in \mathcal{B},\ i = 1,2,$$

and suppose that

$$b_1 \cup \left\{\sum_i b_{1i}\right\} = b_2 \cup \left\{\sum_j b_{2j}\right\},$$

with the sum on the left-hand side of this equation having k terms and the sum on the right having ℓ terms, $2 \leq k \leq 4$ and $2 \leq \ell \leq 4$. We must prove that $k = \ell$.

If $b_1 = b_2$ then, after perhaps reindexing the terms in the sum on the right,

$$\sum_i b_{1i} = \sum_j b_{1j},$$

hence $k = \ell$ since b_1 is linearly independent over F. If $b_1 \neq b_2$, then, after reindexing if necessary, we have

$$b_{11} = \sum_j b_{2j},\ b_{21} = \sum_i b_{1i}, \tag{3.4}$$

$$b_1 \backslash \{b_{11}\} = b_2 \backslash \{b_{21}\}. \tag{3.5}$$

Suppose no index j is 1 in the sum on the right-hand side of the first equation in (3.4). It is then a consequence of (3.4) and (3.5) that, after perhaps reindexing, $b_{11} = \sum_j b_{1j}$, and this can occur only if b_{11} is the sole term in this sum, contrary to the fact that $\ell \geq 2$. Hence an index j in the sum on the right of the first equation in (3.4) must be 1, hence by (3.4) and (3.5) again, after perhaps reindexing the j's,

$$b_{11} = \sum_i b_{1i} + \sum_{j \neq 1} b_{1j},$$

from which it follows that

$$\sum_i b_{1i} = \sum_j b_{1j}.$$

The sum on the left has k terms, the sum on the right has ℓ terms, and so $k = \ell$. QED

For $k = 1$, 2, or 3, let $A(k)$ be the set of ordered pairs

$$A(k) = \{(b, S) :\ b \in \mathcal{B},\ S \subseteq b,\ |S| = k + 1\},$$

and define the surjective map $\rho_k :\ A(k) \to \mathcal{C}(k)$ by

$$\rho_k\left((b, S)\right) = b \cup \left\{\sum_{v \in S} v\right\}.$$

The following lemma provides the required fibration:

Lemma 3.7 *If $k =$ 1, 2, or 3 and $b \cup \left\{\sum_{v \in S} v\right\} \in \mathcal{C}(k)$, then*

$$\left|\rho_k^{-1}\left(b \cup \left\{\sum_{v \in S} v\right\}\right)\right| = k + 2.$$

Proof. Let $b = \{b_1,\ b_2,\ b_3,\ b_4\}$, with the elements of b indexed so that $S = \{b_i :\ i \in [1, k+1]\}$ for $k = 1, 2, 3$. Then by reasoning along lines similar to those

followed in the proof of Lemma 3.6, one can show that for $k = 1, 2$, or 3, $\rho_k^{-1}\left(b \cup \left\{\sum_{v\in S} v\right\}\right)$ is, respectively,

$$\Big\{(b,S),\quad (\{b_1+b_2,\ b_2,\ b_3,\ b_4\},\ \{b_1+b_2,\ b_2\}),\\ (\{b_1,\ b_1+b_2,\ b_3,\ b_4\},\ \{b_1,\ b_1+b_2\})\Big\},$$

$$\Big\{(b,S),\quad \left(\left\{\sum_1^3 b_i,\ b_2,\ b_3,\ b_4\right\},\ \left\{\sum_1^3 b_i,\ b_2,\ b_3\right\}\right),\\ \left(\left\{b_1,\ \sum_1^3 b_i,\ b_3,\ b_4\right\},\ \left\{b_1,\ \sum_1^3 b_i,\ b_3\right\}\right),\\ \left(\left\{b_1,\ b_2,\ \sum_1^3 b_i,\ b_4\right\},\ \left\{b_1,\ b_2,\ \sum_1^3 b_i\right\}\right)\Big\},$$

$$\Big\{(b,S),\quad \left(\left\{\sum_1^4 b_i,\ b_2,\ b_3,\ b_4\right\},\ \left\{\sum_1^4 b_i,\ b_2,\ b_3,\ b_4\right\}\right),\\ \left(\left\{b_1,\ \sum_1^4 b_i,\ b_3,\ b_4\right\},\ \left\{b_1,\ \sum_1^4 b_i,\ b_3,\ b_4\right\}\right),\\ \left(\left\{b_1,\ b_2,\ \sum_1^4 b_i,\ b_4\right\},\ \left\{b_1,\ b_2,\ \sum_1^4 b_i,\ b_4\right\}\right),\\ \left(\left\{b_1,\ b_2,\ b_3,\ \sum_1^4 b_i\right\},\ \left\{b_1,\ b_2,\ b_3,\ \sum_1^4 b_i\right\}\right)\Big\},$$

from which the conclusion of the lemma follows immediately. QED

It is now a consequence of Lemma 3.7 that

$$|A(k)| = (k+2)|\mathcal{C}(k)|,\ k = 1, 2, 3.$$

But we also have that $|A(1)| = 6|\mathcal{B}|$, $|A(2)| = 4|\mathcal{B}|$, and $|A(3)| = |\mathcal{B}|$, and so from Lemma 3.6 we conclude that

$$c(5,5) = |\mathcal{C}_{55}| = 2|\mathcal{B}| + |\mathcal{B}| + \frac{1}{5}|\mathcal{B}| = 2688.$$

Interestingly enough, this calculation shows that all but 315 of the 3003 5-element subsets of $F^4\backslash\{0\}$ contain a basis of F^4.

Returning to our obstruction count in $2^{[1,5]}$, we hence find that

$$|\mathcal{O}_5(5)| = 2520 + 2688 = 5208,$$
$$|\mathcal{O}(5)| = 155 + 5208 = 5363.$$

With regard to the calculation of $|OIP(n)|$, we have unfortunately been unable to make any real progress. If $\mathcal{S} \subseteq 2^{[1,n]}\backslash\{\emptyset\}$ and if we set

$$[\mathcal{S}, +\infty) = \left\{\mathcal{T} \subseteq 2^{[1,n]}\backslash\{\emptyset\} :\ \mathcal{S} \subseteq \mathcal{T}\right\},$$

then

$$OIP(n) = \bigcap_{\mathcal{S}\in\mathcal{O}(n)} 2^{2^{[1,n]}\setminus\{\emptyset\}}\setminus\big(\{\emptyset\}\cup[\mathcal{S},+\infty)\big).$$

Since

$[\mathcal{S},+\infty) \neq [\mathcal{T},+\infty)$ if and only if $\mathcal{S}\neq\mathcal{T}$,

$\displaystyle\bigcap_{\mathcal{S}\in T}[\mathcal{S},+\infty) = \left[\bigcup_{\mathcal{S}\in T}\mathcal{S},+\infty\right)$ for any nonempty subset T of $2^{2^{[1,n]}\setminus\{\emptyset\}}$, and

$\big|[\mathcal{S},+\infty)\big| = 2^{2^n-1-|\mathcal{S}|}$,

we thus deduce from the principle of inclusion and exclusion the following result:

Theorem 3.8 *If $n\geq 2$ is an integer and $OIP(n)$ denotes the set of all subsets of $2^{[1,n]}$ with the odd-intersection property, then*

$$|OIP(n)| = 2^{2^n-1}-1+\sum_{i=3}^{2^n-1} c(i)\cdot 2^{2^n-1-i}, \tag{3.6}$$

where

$$\begin{aligned}
c(i) =&\quad |E(i)|-|O(i)|,\\
E(i) =&\quad \left\{T\subseteq\mathcal{O}(n):\ |T| \text{ is even and } \Big|\bigcup_{\mathcal{S}\in T}\mathcal{S}\Big| = i\right\},\\
O(i) =&\quad \left\{T\subseteq\mathcal{O}(n):\ |T| \text{ is odd and } \Big|\bigcup_{\mathcal{S}\in T}\mathcal{S}\Big| = i\right\},\\
\mathcal{O}(n) =&\quad \text{set of all obstructions contained in } 2^{[1,n]}.
\end{aligned}$$

When $n=2$ or 3, the coefficients in formula (3.6) can be readily calculated by brute force and so we find that

$$|OIP(2)| = 2^3-1-1=6,$$

$$|OIP(3)| = 2^7-1-7\cdot 2^4+0\cdot 2^3+21\cdot 2^2-21\cdot 2+6=63$$

(we are grateful to the referee for correcting an error in a previous version of this calculation). For values of n exceeding 3, the calculation of $|E(i)|$ and $|O(i)|$ becomes rather more complex, and will hence yield to either machine computation or deeper insight into the combinatorics of subsets of $\mathcal{O}(n)$. If nothing else, Theorem 3.8 at least shows how the cardinality of $OIP(n)$ is determined combinatorially from the cardinalities of appropriate subsets of $\mathcal{O}(n)$. We hope to return to these issues in future work.

In closing, we wish to point out an interpretation of the cardinality of $OIP(n)$ that has some interest for number theory. 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 vice-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.

References

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

[2] 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.

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

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

[5] R. Stanley, *Enumerative Combinatorics*, vol. I, Wadsworth, Monterey, 1986.

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

[7] S. Wright, Quadratic nonresidues and the combinatorics of sign multiplication, *Ars Combinatoria* (to appear).

(Received 27 May 2008)