The odd and even intersection properties

Victor Scharaschkin

Department of Mathematics
University of Queensland
St Lucia, Australia, 4072

victors@maths.uq.edu.au

Submitted: Dec 16, 2009; Accepted: Sep 7, 2011; Published: Sep 20, 2011
Mathematics Subject Classification: 05A15, 11A15

Abstract

A non-empty family $\mathcal{S}$ of subsets of a finite set A has the *odd (respectively, even) intersection property* if there exists non-empty $B \subseteq A$ with $|B \cap S|$ odd (respectively, even) for each $S \in \mathcal{S}$. In characterizing sets of integers that are quadratic non-residues modulo infinitely many primes, Wright asked for the number of such $\mathcal{S}$, as a function of $|A|$. We give explicit formulae.

1 Introduction

Let A be a finite non-empty set, let $\mathcal{P}(A)$ denote its powerset, and let $\mathcal{S} \subseteq \mathcal{P}(A)$ be a non-empty collection of subsets of A. (We allow $\emptyset \in \mathcal{S}$, but not $\mathcal{S} = \emptyset$.) We say that $\mathcal{S}$ has the *even intersection property* (EIP) with respect to A if there exists a non-empty set $B \subseteq A$ such that $|B \cap S|$ is even for each $S \in \mathcal{S}$. (The set B is required to be non-empty to avoid triviality.) Similarly, $\mathcal{S} \subseteq \mathcal{P}(A)$ has the *odd intersection property* (OIP) with respect to A if there exists a set $B \subseteq A$ (necessarily non-empty) with $|B \cap S|$ odd for each $S \in \mathcal{S}$. If $|A| = n$, let $d(n)$, respectively $e(n)$, be the number of $\mathcal{S} \subseteq \mathcal{P}(A)$ with the OIP, respectively the EIP. We shall obtain formulae for $d(n)$ and $e(n)$.

It is generally enough to consider these properties when $A = \bigcup \mathcal{S}$. Indeed, in the odd case, if $\mathcal{S}$ has the OIP with respect to some set A (with appropriate $B \subseteq A$, say) then it has the OIP with respect to $\bigcup \mathcal{S}$, since $B' = B \cap \bigcup \mathcal{S}$ still has odd intersection with each $S \in \mathcal{S}$ (in particular, B' is not empty). Thus in the odd case we may take $A = \bigcup \mathcal{S}$ without loss of generality, and may simply speak of $\mathcal{S}$ having the OIP (without specifying A).

This observation does not hold in the even case, since $(B \cap \bigcup \mathcal{S})$ may be empty. However if $A \neq \bigcup \mathcal{S}$ then $\mathcal{S}$ has the EIP trivially, since if $x \in A \setminus \bigcup \mathcal{S}$ then $B = \{x\}$ has empty intersection with each $S \in \mathcal{S}$.

The OIP was introduced by Wright [9], [10] in the following context. If $T \subseteq \mathbb{N}$ is finite and non-empty, there are infinitely many primes p such that every element of T is a quadratic residue mod p [9, Theorem 2.3]. Consider the corresponding statement for quadratic nonresidues:

$(*)$ Every element in T is a quadratic nonresidue mod p, for infinitely many primes p.

Wright [9, Lemma 2.5] gave a combinatorial characterization of the sets T satisfying $(*)$. Namely, for each t in T let S_t be the set of primes dividing the square-free part of t, and let $\mathcal{S}_T = \{S_t \mid t \in T\}$. Then $(*)$ holds for T if and only if $\mathcal{S}_T$ has the OIP. Recently Hu [6] generalized some of these results to dth powers in the ring $\mathbb{F}_q[t]$.

The potential $\mathcal{S}$ with the OIP or EIP are drawn from $\mathcal{P}(\mathcal{P}(A))$, so there are 2^{2^n} sets to consider and exhaustive searching rapidly becomes impossible. Wright [11] found $d(n)$ for $n \leq 3$, and asked for a general formula.

To state our result, recall [4] that the number of d-dimensional subspaces of an m-dimensional $\mathbb{F}_q$-vector space is given by the *q-binomial coefficient*

$$\binom{m}{d}_q = \prod_{j=1}^{d} \frac{q^{m-j+1}-1}{q^j-1}, \qquad 0 \leq d \leq m. \tag{1}$$

(This expression is always an integer.) We show the following.

Theorem 1.1.

$$d(n) = \sum_{i=0}^{n-1} \left[(-1)^{n-i-1} \left(2^{2^i}-1\right) \binom{n}{i}_2 \prod_{j=1}^{n-i} (2^j-1) \right], \tag{2}$$

$$e(n) = 1 + 2\sum_{i=0}^{n-1} \left[(-1)^{n-i-1} \left(2^{2^i-1}-1\right) \binom{n}{i}_2 2^{\binom{n-i}{2}} \right]. \tag{3}$$

The exponent $\binom{n-i}{2}$ in (3) is a regular (not q) binomial coefficient. The sum in (3) can be interpreted as the number of $\mathcal{S}$ with the EIP with $\emptyset \notin \mathcal{S}$, since except for $\mathcal{S} = \{\emptyset\}$, $\mathcal{S}$ has the EIP if and only if $\mathcal{S} \cup \{\emptyset\}$ does.

The symmetry between (2) and (3) becomes more apparent on writing $2^{\binom{n-i}{2}} = \prod_{j=1}^{n-i-1} 2^j$. If we let $\delta = 1$ in the EIP case and $\delta = 0$ in the OIP case we obtain

$$d(n),\ \ e(n) = \delta + \sum_{i=0}^{n-1} \left[(-1)^{n-i-1} \left(2^{2^i}-1-\delta\right) \binom{n}{i}_2 \prod_{j=1}^{n-i-\delta} (2^j-1+\delta) \right]. \tag{4}$$

To prove Theorem 1.1 we identify $\mathcal{P}(A)$ with the vector space $V = \mathbb{F}_2^n$. Equation (2) is then proved in §2 using linear algebra to establish a recurrence relation satisfied by $d(n)$. Equation (3) is derived in §3 by a simple counting argument. Except for some notation the two halves of the proof are independent.

The quantities $d(n)$ and $e(n)$ grow roughly as $2^{(2^{n-1}+n)}$. The first few values are:

n	1	2	3	4	5	6
$d(n)$	1	6	63	2880	1942305	270460574370
$e(n)$	1	7	71	3071	1966207	270499994623

and $e(10) > d(10) > 10^{150}$.

2 The Odd Intersection Property

In this section we prove that $d(n)$ satisfies the following recurrence relation, for $n \geq 2$:

$$d(n) = (2^n - 1)\left(2^{2^{n-1}} - 1 - d(n-1)\right). \tag{5}$$

The formula (2) for $d(n)$ in Theorem 1.1 follows by solving equation (5), with initial condition $d(1) = 1$. The general solution of a first order linear recurrence relation may be found in [3, §1.2] or [7, §2.2].

In what follows, the disjoint union of sets $S_1, \ldots, S_n$ is denoted by $\bigsqcup_{i=1}^n S_i$. To avoid repeating wordy counting arguments, we formalize a trivial observation. If X is a set, $\mathcal{T} \subseteq \mathcal{P}(X)$ and Q is a boolean valued function (predicate) on $\mathcal{P}(X)$, then let $\mathcal{T}^Q = \{S \in \mathcal{T} \mid Q(S) \text{ holds}\}$.

Lemma 2.1. Let X be a non-empty finite set, let $\mathcal{X} = \{X_1, \ldots, X_M\} \subseteq \mathcal{P}(X)$, and suppose $|\mathcal{P}(X_j)^Q| = N$ is independent of j. For $i \geq 0$ define "level sets"

$$\mathcal{Z}_i = \{S \in \mathcal{P}(X)^Q \mid S \subseteq X_j \text{ for exactly } i \text{ of the } X_j\}. \tag{6}$$

Then

$$\Big|\{S \mid S \subseteq X_j \text{ for some } j, \text{ and } Q(S) \text{ holds}\}\Big| = MN - \sum_{i \geq 2}(i-1) \cdot |\mathcal{Z}_i|. \tag{7}$$

Proof Clearly $\Big|\{S \mid S \subseteq X_j \text{ for some } j, \text{ and } Q(S) \text{ holds}\}\Big|$ is just $\Big|\bigcup_{X_j \in \mathcal{X}} \mathcal{P}(X_j)^Q\Big| = \sum_{i \geq 1} |\mathcal{Z}_i|$, while $MN = \Big|\bigsqcup_{X_j \in \mathcal{X}} \mathcal{P}(X_j)^Q\Big| = \sum_{i \geq 1} i\,|\mathcal{Z}_i|$. □

Suppose V is a finite dimensional $\mathbb{F}_2$-vector space and S is a subset of V. The subspace of V generated by S is denoted by $\langle S \rangle$. If $v \in V$, then the set $\{v + s \mid s \in S\}$ is denoted by $v + S$. A codimension one subspace[1] of V is called a *maximal* subspace. The complement $V \setminus W$ of a maximal subspace W of V is called a V*-block.* A non-empty subset of a V-block is called a V*-subblock.*

We define three families of subsets of V. Let $\mathcal{M}(V)$ be the collection of all maximal subspaces of V, $\mathcal{B}(V)$ the collection of all V-blocks, and $\mathcal{C}(V)$ the collection of all V-subblocks:

$$\mathcal{C}(V) = \bigcup_{B \in \mathcal{B}(V)} \mathcal{P}(B) \setminus \{\emptyset\}. \tag{8}$$

[1] The zero space has no maximal subspaces.

In Corollary 2.4 we show that $\mathcal{B}(V)$ forms a symmetric block design, justifying the terminology.

The motivation for introducing these sets is that $|\mathcal{C}(V)| = d(n)$, where $n = \dim V$ (Lemma 2.5). To obtain the recurrence relation (5) we therefore need to consider V-blocks, and also W-blocks for $W \in \mathcal{M}(V)$ (sets of the form $W \setminus X$ where X has codimension one in W). We have the following simple properties.

Lemma 2.2. Let V be a finite dimensional $\mathbb{F}_2$-vector space and suppose $U, W \in \mathcal{M}(V)$.

(a) If $U \neq W$ then $U \cap W \in \mathcal{M}(W)$.

(b) We have $\mathcal{C}(W) \subseteq \mathcal{C}(V)$.

(c) Suppose S is a W or V-subblock. Then $S \subseteq U$ if and only if S is a U-subblock.

Proof

(a) $U + W$ is all of V, so $U/(U \cap W) \simeq (U + W)/W = V/W$ is 1-dimensional.

(b) Suppose $S \in \mathcal{C}(W)$. Say $\emptyset \neq S \subseteq B \subseteq W$ with $W \setminus B \in \mathcal{M}(W)$. Let $x \in V \setminus W$ and $X = \langle x \rangle \oplus (W \setminus B)$. Then $X \in \mathcal{M}(V)$ and $\emptyset \neq S \subseteq V \setminus X$, so $S \in \mathcal{C}(V)$.

(c) By (b) we may assume $S \in \mathcal{C}(V)$. Say $S \subseteq V \setminus X$ for some $X \in \mathcal{M}(V)$. Assume $S \subseteq U$. Then $U \cap X \in \mathcal{M}(U)$ by (a), and $S \subseteq U \setminus (U \cap X)$, so $S \in \mathcal{C}(U)$. The other implication is trivial. $\square$

From now on, assume that the set A is fixed, with $|A| = n \geq 1$ and let $V = \mathbb{F}_2^n$, viewed as a n-dimensional $\mathbb{F}_2$-vector space. Fix the standard basis $\{e_i\}$ of V, where $e_i = (0, 0, \ldots, 1, \ldots, 0)$ has 1 in the ith coordinate and zeros elsewhere. If $x = \sum x_i e_i$ and $y = \sum y_i e_i$ define $x \cdot y = \sum x_i y_i$, viewed as an element in $\mathbb{F}_2$. (Note that the definition of $x \cdot y$ depends on the basis $\{e_i\}$ chosen.) If $S \subseteq V$ is non-empty, let

$$\begin{aligned} S^\circ &= \{v \in V \mid s \cdot v = 0 \text{ for all } s \in S\}, \\ S' &= \{v \in V \mid s \cdot v = 1 \text{ for all } s \in S\}, \end{aligned}$$

and write x° for $\{x\}^\circ$ and x' for $\{x\}'$.

Lemma 2.3.

(a) The maps $x \mapsto x'$, $x \mapsto x^\circ$ give bijections $V \setminus \{0\} \to \mathcal{B}(V)$ and $V \setminus \{0\} \to \mathcal{M}(V)$ respectively.

(b) There are $2^n - 1$ V-blocks each with cardinality 2^{n-1}, and the same is true for maximal subspaces.

(c) Assume $S \in \mathcal{C}(V)$ or $S \in \mathcal{C}(W)$ for some $W \in \mathcal{M}(V)$, and let $k = n - \dim\langle S \rangle$. Then there are exactly 2^k V-blocks containing S, and exactly $2^k - 1$ maximal subspaces U of V containing S. Moreover, in each such U we have $S \in \mathcal{C}(U)$.

Proof Let $S = \{s_1, \ldots, s_m\}$, let $s_i = \sum a_{i,j} e_j$, and form the $m \times n$ matrix $A = (a_{i,j})$ of rank $n-k$. Then $S^\circ = \ker A$, so $\dim S^\circ = k$. In particular, since $U \subseteq (U^\circ)^\circ$ holds for any subspace U, taking $S = U$ we have $\dim U = \dim(U^\circ)^\circ$, so $U = (U^\circ)^\circ$. Thus the maps $\{0, x\} \to x^\circ$ (for $x \neq 0$) and $W \to W^\circ$ give mutually inverse maps between the collection of all 1-dimensional and all maximal subspaces, proving (a) and (b).

Since $\mathcal{C}(W) \subseteq \mathcal{C}(V)$, in (c) we may assume S is a V-subblock. By (a), $S' = \{x \mid S \subseteq x'\}$ is (in bijection with) the set of V-blocks containing S, and hence is non-empty. Furthermore, S' is the set of solutions of $Ax = \underline{1}$ (the vector of all 1's), so $|S'| = |S^\circ| = 2^k$.

Finally, let $U \in \mathcal{M}(V)$. By Lemma 2.2(c) $S \subseteq U$ if and only if $S \in \mathcal{C}(U)$. So the number of $U \in \mathcal{M}(V)$ with $S \in \mathcal{C}(U)$ is just the number of maximal subspaces of V containing S. Such subspaces are in bijection with the maximal subspaces of $V/\langle S \rangle$, a k-dimensional space, containing $2^k - 1$ maximal subspaces by (b). □

Note that (c) above implies that if we know that S is contained in exactly 2^k V-blocks or $2^k - 1$ maximal subspaces, we can deduce that $\dim\langle S \rangle = k$. We observe in passing that $S \subseteq T^\circ$ if and only if $T \subseteq S^\circ$, so the $(-)^\circ$-operation forms a Galois connection (with itself) [8, Ch. 6].

The next result is not needed in our proof, but motivates the terminology. See [5, Ch. 14] or [2, Ch. 1.5] for definitions.

Corollary 2.4. For $n \geq 2$, the set $\mathcal{B}(V)$ forms a symmetric block design on the set $V \setminus \{0\}$, with $(v, k, \lambda) = (2^n - 1,\ 2^{n-1},\ 2^{n-2})$.

Proof This follows on putting $S = \{x\}$ and $S = \{x, y\}$ with $x \neq y$, $x, y \neq 0$ in Lemma 2.3(c), since S' is clearly non-empty in each case. □

We apply these results to the OIP. We identify $\mathcal{P}(A)$ with V by mapping a subset $T \subseteq A = \{a_1, \ldots, a_n\}$ to $v_T = \sum_{i=1}^n \chi_T(a_i) e_i$, where $\chi_T \colon A \to \mathbb{F}_2$ is the characteristic function of T. A collection $\mathcal{S}$ of subsets of A corresponds to a subset $S \subseteq V$. Those collections $\mathcal{S}$ with the OIP correspond to V-subblocks:

Lemma 2.5. Under the identification $\mathcal{P}(A) \simeq V$ a collection of subsets of A has the OIP if and only if it corresponds to an element of $\mathcal{C}(V)$. Thus

$$d(n) = |\mathcal{C}(V)|. \tag{9}$$

Proof If S and T are subsets of A, then $v_S \cdot v_T \equiv |S \cap T| \pmod 2$. Thus for S a non-empty subset of V, S has the OIP $\iff$ there exists $x \in V$ with $s \cdot x = 1$ for all $s \in S$ $\iff$ $S \subseteq x'$ for some $x \in V \setminus \{0\}$ $\iff$ $S \subseteq B$ for some $B \in \mathcal{B}(V)$. □

The identification $T \mapsto v_T$ depends on the basis $\{e_i\}$, as do the individual sets x'. However the collection $\{x' \mid x \neq 0\} = \mathcal{B}(V)$ is basis independent, as is equation (9). Thus for example $d(n-1) = |\mathcal{C}(W)|$ for any $W \in \mathcal{M}(V)$.

We now prove the recursion relation (5) for $d(n)$.

Proof (Of (2)) For $k \geq 1$ define

$$\mathcal{V}_k = \{S \in \mathcal{P}(V) \mid S \neq \emptyset \text{ is a subset of exactly } 2^k\ V\text{-blocks}\}. \tag{10}$$

By Lemma 2.3(c)

$$\mathcal{V}_k = \{S \in \mathcal{P}(V) \mid S \text{ is a } W\text{-subblock for exactly } 2^k - 1 \; W \in \mathcal{M}(V)\}. \tag{11}$$

We apply Lemma 2.1 twice, with $X = V$. First take $\mathcal{X} = \mathcal{B}(V)$, and let $Q(S)$ be the property $S \neq \emptyset$. By Lemma 2.3 the set $\mathcal{Z}_i$ is empty except if $i = 2^k$, and $\mathcal{Z}_{2^k} = \mathcal{V}_k$. Applying equation (9) gives

$$d(n) = (2^n - 1)(2^{2^{n-1}} - 1) - \sum_{k \geq 1} (2^k - 1)|\mathcal{V}_k|. \tag{12}$$

Next take $\mathcal{X} = \mathcal{M}(V)$, and let $Q(S)$ hold if and only if $S \in \mathcal{C}(W)$ for some $W \in \mathcal{M}(V)$. By Lemma 2.2(c) if $Q(S)$ holds and $S \subseteq X_j \in \mathcal{X}$ then $S \in \mathcal{C}(X_j)$, so $\mathcal{P}(X_j)^Q = \mathcal{C}(X_j)$, and hence $|\mathcal{P}(X_j)^Q| = d(n-1)$. Furthermore by Lemma 2.3 the set $\mathcal{Z}_i$ is empty unless $i = 2^k - 1$ for some $k \geq 1$, and $\mathcal{Z}_{2^k - 1} = \mathcal{V}_k$. This gives

$$\sum_{k \geq 1} (2^k - 1)|\mathcal{V}_k| = (2^n - 1) d(n-1). \tag{13}$$

Equation (5) follows from (12) and (13). □

3 The Even Intersection Property

In this section we establish equation (3) for $e(n)$. Let $g(d)$ be the number of subsets of a d-dimensional $\mathbb{F}_2$-vector space U that generate U. Under the identification $\mathcal{P}(A) \simeq V$,

$$S \subseteq V \text{ has the EIP} \iff \emptyset \neq S \subseteq W \quad \text{for some} \quad W \in \mathcal{M}(V). \tag{14}$$

Thus a non-empty set $S \subseteq V$ does not have the EIP if and only if it generates V, so $g(n) = 2^{2^n} - 1 - e(n)$ for $n \geq 1$. Since every subset $S \subseteq V$ gives rise to a subspace $U = \langle S \rangle$ in which (of course) S generates U, summing over all generating subsets of all subspaces of V gives

$$\sum_{d=0}^{n} \binom{n}{d}_2 g(d) = 2^{2^n}. \tag{15}$$

We solve for $g(n)$. Taking $n = 1, 2, \ldots, m$ successively in equation (15) and subtracting the $d = 0$ terms gives rise to the linear system

$$B \begin{pmatrix} g(1) \\ g(2) \\ \vdots \\ g(m) \end{pmatrix} = \begin{pmatrix} 2^{2^1} - 2 \\ 2^{2^2} - 2 \\ \vdots \\ 2^{2^m} - 2 \end{pmatrix}, \tag{16}$$

where B is the $m \times m$ matrix in the next lemma.

Lemma 3.1. Let B be the lower triangular $m \times m$ matrix with (i,j) entry $\binom{i}{j}_2$ if $i \geq j$, and remaining entries 0. Then

$$(B^{-1})_{jk} = \begin{cases} (-1)^{j-k}\, 2^{\binom{j-k}{2}} \binom{j}{k}_2, & \text{if } j \geq k \\ 0, & \text{otherwise.} \end{cases} \tag{17}$$

Proof Let C be the $m \times m$ matrix with entries given by the right hand side of (17). Clearly BC is lower triangular, with 1's on the diagonal, so it remains to show $(BC)_{ik} = 0$ for $i > k$. This follows from Cauchy's q-binomial Theorem [1, equation 10.0.9]:

$$\sum_{h=0}^{N} q^{\binom{h}{2}} \binom{N}{h}_q t^h = \prod_{h=0}^{N-1} (1 + q^h t), \tag{18}$$

and the identity $\binom{i}{j}_2 \binom{j}{k}_2 = \binom{i}{k}_2 \binom{i-k}{j-k}_2$. We have

$$(BC)_{ik} = \sum_{j=k}^{i} \binom{i}{j}_2 \binom{j}{k}_2 (-1)^{j-k}\, 2^{\binom{j-k}{2}} = \binom{i}{k}_2 \sum_{h=0}^{i-k} 2^{\binom{h}{2}} \binom{i-k}{h}_2 (-1)^h = 0, \tag{19}$$

where the last step follows from writing $h = j - k$ and applying (18) with $t = -1$ and $q = 2$. □

Applying Lemma 3.1 to equation (16) gives (3), and completes the proof in the even case.

References

[1] G. E. Andrews, R. Askey, R. Roy, Special Functions, Cambridge University Press, 2000.

[2] C. Colbourn, J. Dinitz (Eds.), The CRC Handbook of Combinatorial Designs, CRC Press, 1996.

[3] S. Elaydi, An Introduction to Difference Equations, third ed., Springer, 2005.

[4] J. Goldman, G–C. Rota, The number of subspaces of a vector space, Recent Progress in Combinatorics, Ed. W. T. Tutte, Academic Press (1969) 75–83.

[5] R. Graham, M. Grötschel, L. Lovász (Eds.), Handbook of Combinatorics, Vol. 1, MIT Press, 1995.

[6] S. Hu, A note on the dth power residue symbol of $\mathbb{F}_q[t]$, J. Number Theory 128 (2008) 2655–2662.

[7] R. Mickens, Difference Equations, Theory and Applications, second ed., Chapman & Hall, 1991.

[8] S. Roman, Field Theory, second ed., Springer, 2006.

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

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

[11] S. Wright, Some Enumerative Combinatorics Arising From a Problem on Quadratic Nonresidues, Australasian J. Combinatorics, 44 (2009) 301–315.