ENUMERATION PROBLEMS FOR AFFINE MAGIC SQUARES

CHRISTOPHER J. HENRICH

Abstract. Affine magic squares are a class of magic squares, of prime-power order. An affine magic square is determined by an affine isomorphism of a finite vector space. This paper answers the question, how many affine magic squares there are of a given order.

Corrected version, June 15, 2011

1. Introduction

A magic square of order n is an arrangement of n^2 numbers $\{0, \ldots, n^2-1\}$ in an $n \times n$ square, so that each row, column, or diagonal adds up to the sum S. Because $S = 0 + \cdots + (n^2-1)$, we have

$$S = n(n^2-1)/2 \; .$$

(This definition, starting from 0 rather than 1, is not traditional, but it will be more convenient in what follows.) If the diagonals are not required to have the same "magic" sum, then the square is said to be semi-magic. In [5] a class of magic squares, called affine magic squares, was introduced.[1] That paper concentrates on squares of order 4, but the principle is easily extended to squares of order p^m for prime p. One may then ask how many magic squares there are for a given order. The solution of this problem is given here, as an application of the generalized principle of inclusion-exclusion [9] and the techniques of Joni and Rota [7].

2. Definition of affine magic squares

The definition is based on the finite vector space $\mathbf{F}_p^{2m}$. The standard ordered basis of $\mathbf{F}_p^{2m}$ will be denoted by $(\mathsf{e}_1, \ldots, \mathsf{e}_{2m})$. The dual ordered basis of $(\mathbf{F}_p^{2m})^*$ will be denoted by $(f_1, \ldots, f_{2m})$.

The natural map $\mathbb{Z} \to \mathbf{F}_p$ sending n to "n modulo p" will be denoted μ. It has a left inverse, $\nu : \mathbf{F}_p \to \{0, \ldots, p-1\}$. We will not be infinitely scrupulous about distinguishing a numeral, such as 0, from $\mu(0)$.

The **square frame** of order n is

$$S(n) = \{0, \ldots, n-1\} \times \{0, \ldots, n-1\} \; ;$$

elements of $S(n)$ are **cells**. A **square** of order n is a map from $S(n)$ to $\{0, \ldots, n^2-1\}$. We define the **position map** $\mathbf{P} : \mathbf{F}_p^{2m} \to S(p^m)$ by

$$\mathbf{P}(\Sigma_{i=1}^{2m} x_i \mathsf{e}_i) = (\Sigma_{i=1}^{m} \nu(x_i) p^{m-i}, \; \Sigma_{i=1}^{m} \nu(x_{m+i}) p^{m-i}) \; .$$

[1] See also `http://mathinteract.com`.

Then the rows and columns of the square are images under $\mathbf{P}$ of the affine subspaces parallel to

$$\mathbf{E}_R =< \mathsf{e}_{m+1}, \ldots, \mathsf{e}_{2m} > \tag{2.1}$$

and

$$\mathbf{E}_C =< \mathsf{e}_1, \ldots, \mathsf{e}_m > \tag{2.2}$$

respectively. The principal diagonal is the image of the linear subspace

$$\mathbf{E}_+ =< \mathsf{e}_1 + \mathsf{e}_{m+1}, \ldots, \mathsf{e}_m + \mathsf{e}_{2m} > \tag{2.3}$$

while the opposite diagonal is the image of an affine subspace parallel to

$$\mathbf{E}_- =< \mathsf{e}_1 - \mathsf{e}_{m+1}, \ldots, \mathsf{e}_m - \mathsf{e}_{2m} > \ . \tag{2.4}$$

When $p = 2$, of course $\mathbf{E}_+ = \mathbf{E}_-$. As we shall see, this coincidence makes the theory of magic squares of order 2^m slightly different from that for odd prime powers.

We define the **value map** $\mathbf{V} : \mathbf{F}_p^{2m} \to \{0, \ldots, p^{2m} - 1\}$ by

$$\mathbf{V}(\Sigma_{i=1}^{2m} x_i \mathsf{e}_i) = \Sigma_{i=1}^{2m} \nu(x_i) p^{2m-i} \ . \tag{2.5}$$

With these definitions, any function $\Phi : \mathbf{F}_p^{2m} \to \mathbf{F}_p^{2m}$ determines a square of order p^m, not necessarily magic: it assigns the number $\mathbf{V}(\Phi(\mathsf{x}))$ to the cell $\mathbf{P}(\mathsf{x})$.

Definition 2.1. A square of order p^m is an **affine square** if it is determined by a non-singular affine function $\mathsf{A} : \mathbf{F}_p^{2m} \to \mathbf{F}_p^{2m}$. The **digit coordinates** of the square are the functions $A_j = f_j \circ \mathsf{A}$. The **linear parts** of A and A_j are $\mathsf{A}^L : \mathsf{x} \mapsto \mathsf{Ax} - \mathsf{A0}$ and $A_j^L = f_j \circ \mathsf{A}^L$.

Definition 2.2. Let $\mathbf{E}$ be a vector subspace of $\mathbf{F}_p^{2m}$; then the affine square $\mathbf{S}$ determined by the affine isomorphism A is **uniform** for the subspace $\mathbf{E}$ if each digit coordinate of A is nonconstant on $\mathbf{E}$.

We shall also say that $\mathbf{E}$, and the affine subspaces parallel to it, are uniform for that $\mathbf{S}$. An equivalent condition is that each A_j^L, restricted to $\mathbf{E}$, should be non-zero.

It is elementary, but helpful, to note that these statements are equivalent for an affine mapping A of $\mathbf{F}_p^{2m}$ into itself:

(a) A is bijective;
(b) A^L is an isomorphism;
(c) $\{A_j^L \mid j = 1, \ldots, 2m\}$ is a basis of $(\mathbf{F}_p^{2m})^*$.

Proposition 2.3. *Let* $\mathbf{E}$ *be a vector subspace of* $\mathbf{F}_p^{2m}$*, with* $\dim \mathbf{E} = b$*; let* $\mathbf{E}$ *be uniform for the affine square* $\mathbf{S}$*. If* $\mathbf{E}'$ *is any affine space parallel to* $\mathbf{E}$*, and* A *is the affine map that determines* $\mathbf{S}$*, then*

$$\sum_{\mathsf{x} \in \mathbf{E}'} \mathbf{V}(\mathsf{Ax}) = p^b (p^{2m} - 1)/2 \ .$$

Proof. By hypothesis, each digit coordinate A_j is a non-constant affine function from $\mathbf{E}$ to $\mathbf{F}_p$; likewise from $\mathbf{E}'$ to $\mathbf{F}_p$. Consequently, it takes the values $0, \ldots, p-1$ each p^{b-1} times on $\mathbf{E}'$. The contribution of $A_j\mathsf{x}$ to the sum of $\mathbf{V}(\mathsf{Ax})$ over $\mathbf{E}'$ is therefore $p^{2m-j+b}(p-1)/2$. Thus the sum of $\mathbf{V}(\mathsf{Ax})$ over $\mathbf{E}'$ is

$$\sum_{j=1}^{2m} p^{2m-j+b}(p-1)/2 = p^b(p^{2m} - 1)/2 \ .$$

□

When a subspace $\mathbf{E}$ is not uniform for a given square, the situation becomes more complicated. We can, however, say this:

Proposition 2.4. *Let $\mathbf{E}$ be a vector subspace of $\mathbf{F}_p^{2m}$ with $\dim \mathbf{E} = b$. Let J be a subset of $\{1, \dots, 2m\}$, and suppose that for a given affine square $\mathbf{S}$, the digit coordinate A_j is constant on $\mathbf{E}$ precisely when $j \in J$. Let $\mathsf{x} \in \mathbf{F}_p^{2m}$, and let $v_j = A_j(\mathsf{x})$, $j = 1, \dots, 2$. Let $\mathbf{E}'$ be the affine space, parallel to $\mathbf{E}$, including x. Then the sum of the values at positions in $\mathbf{S}$ corresponding to the points of $\mathbf{E}'$ is*

$$p^b(p^{2m} - 1)/2 + \sum_{j \in J} p^{b+2m-j}(v_j - (p-1)/2)\ . \tag{2.6}$$

Proof. If $j \notin J$, then the contribution of A_j to this sum is, as in the previous proof, $p^{2m-j+b}(p-1)/2$. If, on the other hand, $j \in J$, then A_j is constant on $\mathbf{E}'$ and equal there to v_j. The conclusion follows immediately. □

Definition 2.5. A **weakly uniform affine square** is an affine square for which $\mathbf{E}_R$ and $\mathbf{E}_C$ are uniform. A **strongly uniform affine square** is a weakly uniform affine square for which, in addition, $\mathbf{E}_+$ and $\mathbf{E}_-$ are uniform.

Proposition 2.6. *Let $\mathbf{S}$ be a weakly uniform affine square. Then $\mathbf{S}$ is a semimagic square of order p^m (see §1). If p is odd, and the central cell of $\mathbf{S}$ contains $(p^{2m}-1)/2$, then $\mathbf{S}$ is a magic square.*

Proof. The first statement follows immediately from the definitions and from Proposition 2.3. For the second statement, let A be the affine map which generates $\mathbf{S}$. Let x_0 be the element of $\mathbf{F}_p^{2m}$ whose coordinates are all $(p-1)/2$; then $\mathbf{P}(\mathsf{x}_0)$ is the central cell of the square. By hypothesis, $\mathbf{V}(\mathsf{A}\mathsf{x}_0) = (p^{2m} - 1)/2$, that is, at x_0 the digit coordinates take the value $v_j = A_j(\mathsf{x}_0) = (p-1)/2$. Proposition 2.4 applies to show that the sum of the values is $p^m(p^{2m} - 1)/2$, for any m-dimensional affine subspace passing through x_0; in particular this is the case for the subspaces parallel to $\mathbf{E}_+$ and $\mathbf{E}_-$ that are the two unbroken diagonals. □

Proposition 2.7. *Let $\mathbf{S}$ be a strongly uniform affine square. Then $\mathbf{S}$ is a magic square of order p^m. If $m = 1$ and p is odd, then $\mathbf{S}$ is pandiagonal.*

Proof. That $\mathbf{S}$ is magic follows directly from the hypothesis and from Proposition 2.3. The second statement also follows, when we observe that the broken diagonals parallel to the main (resp. the minor) unbroken diagonal of a square of order p correspond to the affine subspaces parallel to $\mathbf{E}_+$ (resp. $\mathbf{E}_-$). □

Definition 2.8. An **affine magic square** is a weakly unform affine square which is also a magic square.

Having arrived at this definition, we can recognize its precursors. Many of them apply to the case that $m = 1$, but they generalize from a prime p to an odd number n. The ring $\mathbb{Z}/n\mathbb{Z}$ replaces the field $\mathbf{F}_p$. Kraïtchik ([8] pp. 157-167) describes the resulting method. According to Stark ([10], chap. 4), this method was also discovered by D. H. Lehmer in 1929; he called it the "uniform step method." Two classical methods for constructing odd-order magic squares, known as those of De la Loubère and Barchet de Méziriac, are special cases. Benson and Jacoby ([2], pp. 43-58) have a similar method. It uses a more general "value mapping," that is,

it allows an arbitrary correspondence between the elements of $\mathbb{Z}/n\mathbb{Z}$ and integers from 0 to $p-1$.

Some methods of constructing squares of even order, when applied to orders 4 and 8, can be seen to give affine squares; consider, for example, [2] pp. 6-7 and 70-77. In [8], pp. 182-183, there is a method which turns out to give all the affine magic squares of order 4.

Finally, Adler [1] has presented essentially the same definition of affine magic squares, and generalized it to magic cubes, tesseracts, and so on.

Proposition 2.7 gives sufficient conditions for an affine square to be magic. The converse result, giving necessary conditions, is more complicated.

Lemma 2.9. *Let ϕ be a non-zero affine function $\mathbf{F}_p^{2m} \to \mathbf{F}_p$, and let $\mathbf{E}$ be a vector subspace of $\mathbf{F}_p^{2m}$ on which ϕ is constant. Then ϕ is constant on every affine subspace $\mathbf{E}'$ parallel to $\mathbf{E}$, and it assumes each value in $\{0, \ldots, p-1\}$ on equally many such subspaces.*

Proof. The linear part of ϕ is 0 on $\mathbf{E}$; from this it folows that ϕ is constant on each $\mathbf{E}'$. The set of all these subspaces constitutes the quotient vector space, $\mathbf{F}_p^{2m}/\mathbf{E}$, on which ϕ determines a non-zero affine function. This function takes each possible value an equal number of times. □

Proposition 2.10. *Let $\mathbf{S}$ be an affine square which is semimagic. Then $\mathbf{S}$ is weakly uniform.*

Proof. In Proposition 2.4, let $\mathbf{E}$ be either $\mathbf{E}_R$ or $\mathbf{E}_C$. Suppose $\mathbf{E}$ is not uniform for $\mathbf{S}$; then (2.6) gives the sum of values on a typical row or column. Now v_j, considered as an ordinary integer, satisfies $0 \le v_j \le p-1$; therefore (2.6) will have the desired value $p^m(p^{2m}-1)/2$ if and only if $v_j = (p-1)/2$ for all $j \in J$. But if A_j is constant on $\mathbf{E}$, then by Lemma 2.9 the value of v_j cannot be the same on every affine subspace parallel to $\mathbf{E}$. We infer that all the A_j must be uniform on $\mathbf{E}_R$ and $\mathbf{E}_C$, and conclude that $\mathbf{S}$ is weakly uniform. □

Proposition 2.11. *Let $\mathbf{S}$ be an affine magic square of order 2^m. Then $\mathbf{S}$ is strongly uniform.*

Proof. By Proposition 2.10, $\mathbf{S}$ is weakly uniform. Suppose $\mathbf{S}$ were not uniform for $\mathbf{E}_+$. Then (2.6) would apply to $\mathbf{E}' = \mathbf{E}_+ = \mathbf{E}_-$; for the sum to agree with the magic value of $p^b(p^{2m}-1)/2$, we would need v_j equal to $1/2$, which is clearly impossible. We thus conclude that $\mathbf{E}_+ = \mathbf{E}_-$ is uniform for $\mathbf{S}$ □

Proposition 2.12. *Let $\mathbf{S}$ be an affine magic square of order p^m where p is odd, and assume that $\mathbf{S}$ is semimagic. Let x_0 be the element of $\mathbf{F}_p^{2m}$ which is mapped to the central cell of the square. Let $(A_1, \ldots, A_{2m})$ be the digit coordinates of $\mathbf{S}$; define*

$$J_+ = \{j \mid A_j \text{ is constant on } \mathbf{E}_+\}$$

and

$$J_- = \{j \mid A_j \text{ is constant on } \mathbf{E}_-\}\,.$$

Then $\mathbf{S}$ is magic if and only if $A_j(\mathsf{x}_0) = (p-1)/2$ for every j in $J_+ \cup J_-$.

Proof. As in the previous two propositions, we apply (2.6) twice, letting $\mathbf{E}'$ be each of the diagonals passing through the central cell. □

3. Enumeration problems for affine squares

How many linear subspaces are uniform for a particular affine square? How many affine squares are uniform for a given set of linear subspaces? Finally, how many affine magic squares are there of a given order? These questions can be answered by applying the work of Joni and Rota[7] on the number of bases $\{\phi_1, \ldots, \phi_n\}$ of a finite vector space $\mathbf{V}$, subject to the constraint that none of the ϕ_i belong to a specified subset of $\mathbf{V}$. To apply this work, we let $\mathbf{V} = (\mathbf{F}_p^{2m})^*$, and use the fact that the linear parts of the digit coordinates for an affine square are a basis of $\mathbf{V}$; moreover, the square is uniform for a given vector subspace $\mathbf{E}$ of $\mathbf{F}_p^{2m}$ if and only if none of the basis elements lie in $\mathbf{E}^\perp \subseteq \mathbf{V}$.

In this section, we present the ingredients of the solution, i.e., elementary combinatorial facts about finite vector spaces and the theorem of Joni and Rota. The succeeding sections take on successively more general and complicated parts of the problem. To begin, in §4, we find how many affine squares are uniform for a single vector subspace; a closely related question is the number of vector subspaces that are uniform for a given affine square. In §5, we count the squares that are uniform for two subspaces which span the whole of $\mathbf{F}_p^{2m}$; in particular, this gives us the number of weakly uniform affine squares. The problem of enumerating the strongly affine magic squares is more complicated, because it deals with subspaces of $(\mathbf{F}_p^{2m})^*$ that are not independent. For this reason, in §6 we deal first with squares that are uniform for one diagonal subspace, and then with strongly affine magic squares. Finally, for general affine magic squares of odd order, from Proposition 2.12 we see that the condition of being strongly uniform must be weakened; we complete the task of enumeration in §7.

First, let us relate the enumeration of affine squares to that of bases of $(\mathbf{F}_p^{2m})^*$.

Proposition 3.1. *Let Φ be a class of bases of $(\mathbf{F}_p^{2m})^*$; let $|\Phi|$ denote the number of elements in Φ. Then the number of affine functions A such that the linear parts of the digit coordinates of A form an element of Φ is*

$$(2m)!p^{2m}|\Phi| \; . \tag{3.1}$$

Proof. An affine map A is determined by (i) the basis of $(\mathbf{F}_p^{2m})^*$ formed of the linear parts of the digit coordinates of A; (ii) an arbitrary permutation of that basis; (iii) the image of 0 under A. The factors on the right-hand side of (3.1) are accounted for by (ii), (iii), and (i) respectively. □

Next, some facts about finite-dimensional vector spaces over $\mathbf{F}_p$. These are well known; references include [4] and [6] pp. 65-67. We shall use the following notations:

$$P(n) = (p^n - 1)(p^{n-1} - 1) \cdots (p - 1) \; ; \tag{3.2}$$

$$\begin{bmatrix} n \\ b \end{bmatrix} = \frac{P(n)}{P(b)P(n-b)} \; . \tag{3.3}$$

In the notation of q-binomial coefficients[11], $P(n) = (p-1)^n [n]_p!$ and $\begin{bmatrix} n \\ b \end{bmatrix} = \begin{bmatrix} n \\ b \end{bmatrix}_p$.

Definition 3.2. Let $\mathbf{V}$ be a vector space, and let K be a linearly independent set of members of $\mathbf{V}$. Let $j \geq 0$. Then a j-**frame extending** K is a sequence $(\mathsf{v}_1, \ldots, \mathsf{v}_j)$ such that $K \cup \{\mathsf{v}_1, \ldots, \mathsf{v}_j\}$ is linearly independent.

Proposition 3.3. *Let $\mathbf{V}$ be a vector space of dimension n over $\mathbf{F}_p$. Let K be a linearly independent set of k elements of $\mathbf{V}$, and let $0 \leq j \leq n - k$. Then*

(a) *the number of j-frames extending K is*

$$F(n,k,j) = \frac{p^{kj+j(j-1)/2}P(n-k)}{P(n-k-j)} \; ; \tag{3.4}$$

(b) *the number of bases of $\mathbf{V}$ containing K as a subset is*

$$B(n,k) = \frac{F(n,k,n-k)}{(n-k)!} = \frac{p^{(n-k)(n+k-1)/2}P(n-k)}{(n-k)!} \; ; \tag{3.5}$$

(c) *the number of linearly independent sets of j elements of $\mathbf{V}$ is*

$$\frac{F(n,0,j)}{j!} = \frac{p^{j(j-1)/2}P(n)}{P(n-j)j!} \; ;$$

(d) *the number of bases of $\mathbf{V}$ is*

$$\frac{F(n,0,n)}{n!} = \frac{p^{n(n-1)/2}P(n)}{n!} \; .$$

Proof. Let $(v_1,\dots,v_j)$ be a typical j-frame extending K. Because v_1 must not belong to the k-dimensional subspace spanned by K, there are $p^n - p^k$ choices for v_1. Similarly, given v_1 there are $p^n - p^{k+1}$ choices for v_2. The number of j-frames extending K is thus

$$(p^n - p^k)(p^n - p^{k+1}) \cdots (p^n - p^{k+j-1})$$

which can be rearranged to give (3.4). The other three parts of the proposition are merely special cases which will be useful later. □

Proposition 3.4. *Let $\mathbf{V}$ be as above. Then the number of j-dimensional subspaces of $\mathbf{V}$ is $\begin{bmatrix} n \\ j \end{bmatrix}$.*

Proof. Every linearly independent set of j vectors in $\mathbf{V}$ spans a j-dimensional subspace. The number of such sets is given by Proposition 3.3c as

$$p^{j(j-1)/2}P(n)/(P(n-j)j!) \; .$$

From part d of the same proposition, the number of bases of a given j-dimensional subspaces is $p^{j(j-1)/2}P(j)/j!$. □

Proposition 3.5. *Let $\mathbf{V}$ be as above, and let $\mathbf{W}$ be a subspace of dimension k. Let $\mathbf{A}$ be a j-dimensional subspace of $\mathbf{V}/\mathbf{W}$. Then the number of j-dimensional subspaces $\mathbf{B}$ of $\mathbf{V}$ such that $\mathbf{A}$ is the image of $\mathbf{B}$ is p^{jk}.*

Proof. Let π denote the projection of $\mathbf{V}$ onto $\mathbf{V}/\mathbf{W}$. Let $\{\mathsf{a}_1,\dots,\mathsf{a}_j\}$ be a basis of $\mathbf{A}$. Each subspace $\mathbf{B}$ of the required kind has a unique basis $\{\mathsf{b}_1,\dots,\mathsf{b}_j\}$ such that $\pi\mathsf{b}_\iota = \mathsf{a}_\iota$, and conversely each set of solutions of the latter equations gives a basis of such a subspace. But for each a_ι there are p^k solutions of $\pi\mathsf{b}_\iota = \mathsf{a}_\iota$. □

Proposition 3.6. *Let $\mathbf{V}$ and $\mathbf{W}$ be as in Proposition 3.5. The number of j-dimensional subspaces $\mathbf{A}$ of $\mathbf{V}$ such that $\mathbf{A} \cap \mathbf{W} = \{\mathsf{0}\}$ is*

$$v(n,k,j) = p^{kj} \begin{bmatrix} n-k \\ j \end{bmatrix} \; . \tag{3.6}$$

Proof. This is a consequence of the two previous propositions. The second factor on the right side of equation (3.6) is the number of j-dimensional subspaces of the $(n-m)$-dimensional space $\mathbf{V}/\mathbf{W}$; and the first factor is the number of ways of lifting such a subspace to a j-dimensional subspace of $\mathbf{V}$. □

Proposition 3.7. *With the notation of Proposition 3.6, let* $\mathbf{B}$ *be a subspace of* $\mathbf{W}$ *of dimension* b*. Suppose* $b \le j \le n-k+b$*. Then the number of* j*-dimensional subspaces* $\mathbf{A}$ *of* $\mathbf{V}$ *such that* $\mathbf{A} \cap \mathbf{W} = \mathbf{B}$ *is* $v(n-b, k-b, j-b)$*.*

Proof. Consider the quotient space $\mathbf{V}/\mathbf{B}$. The image $\mathbf{A}/\mathbf{B}$ of $\mathbf{A}$ determines $\mathbf{A}$; and $\mathbf{A}/\mathbf{B}$ is a subspace of dimension $j-b$ whose intersection with the $(n-b)$-dimensional $\mathbf{W}/\mathbf{B}$ is $\{0\}$. □

Proposition 3.8. *Let* $\mathbf{V}$ *be as above; let* $\mathbf{B}$ *be a subspace of dimension* b*. Let* a_1 *and* a_2 *satisfy* $a_1 \ge b$*,* $a_2 \ge b$*, and* $a_1 + a_2 \le n + b$*. Then the number of pairs* $(\mathbf{A}_1, \mathbf{A}_2)$*, where* $\mathbf{A}_i$ *is a subspace of* $\mathbf{V}$ *of dimension* a_i *and* $\mathbf{A}_1 \cap \mathbf{A}_2 = \mathbf{B}$*, is*

$$w(n, b, a_1, a_2) = p^{(a_1-b)(a_2-b)} \begin{bmatrix} n-b \\ a_1-b \end{bmatrix} \begin{bmatrix} n-a_1 \\ a_2-b \end{bmatrix} . \tag{3.7}$$

Proof. $\mathbf{A}_1$ is determined by its image in $\mathbf{V}/\mathbf{B}$, that is, by a subspace of dimension $a_1 - b$ in a vector space of dimension $n - b$. The number of such subspaces, by Proposition 3.4, is $\begin{bmatrix} n-b \\ a_1-b \end{bmatrix}$. For a fixed choice of $\mathbf{A}_1$, the number of choices of $\mathbf{A}_2$ is given by Proposition 3.7 as

$$v(n-b, a_1-b, a_2-b) = p^{(a_1-b)(a_2-b)} \begin{bmatrix} n-a_1 \\ a_2-b \end{bmatrix} .$$

□

We use the following theorem of Joni and Rota.

Theorem 3.9. *(See* [7]*, Theorem 3.1.) Let* $\mathbf{V}$ *be a vector space of dimension* n *over* $\mathbf{F}_p$*. Let* S *be a subset of* $\mathbf{V}$*. Let* $W_k(S)$ *denote the number of linearly independent sets of* k *elements of* S*, and let* $B(n,k)$ *denote the number of bases of* $\mathbf{V}$ *containing a given linearly independent set of* k *elements, given in* (3.5)*. Then the number* $r_0(S)$ *of bases of* $\mathbf{V}$ *which contain no elements of* S *is*

$$r_0(S) = \sum_{k=0}^{n} (-1)^k W_k(S) B(n,k) . \tag{3.8}$$

4. One uniform subspace

Proposition 4.1. *Let* $\mathbf{V}$ *be a vector space of dimension* n *over* $\mathbf{F}_p$*. Let* S *be a vector subspace of* $\mathbf{V}$*, of dimension* b*. Then the number of bases of* $\mathbf{V}$ *which do not contain any elements of* S *is*

$$A(n,b) = \sum_{k=0}^{b} (-1)^k F(b,0,k) B(n,k)/k! .$$

Proof. This is an application of Theorem 3.9. The value of $B(n,k)$ is given by Proposition 3.3b; to find the desired number it is sufficient to find $W_k(S)$. But this is given by Proposition 3.3a. □

Proposition 4.2. *The number of nonsingular affine maps* A *on* $\mathbf{F}_p^{2m}$ *for which a given linear subspace* $\mathbf{E}$ *is uniform is*

$$(2m)! p^{2m} A(2m, 2m - \dim \mathbf{E}) .$$

Proof. An affine map A satisfies the given condition if and only if no member of the associated basis of $(\mathbf{F}_p^{2m})^*$ belongs to $\mathbf{E}^\perp$, which is a linear subspace of dimension $2m - \dim \mathbf{E}$. This this proposition follows from the previous one, together with Proposition 3.1. □

We have counted the affine maps which are uniform for a given subspace; now, let us determine how many subspaces are uniform for a given map.

Proposition 4.3. *Let $\mathbf{V}$ be a vector space of dimension n over $\mathbf{F}_p$; let $\{\phi_1, \ldots, \phi_n\}$ be a basis of $\mathbf{V}^*$. Then the number of b-dimensional subspaces $\mathbf{E}$ of $\mathbf{V}$ such that none of the ϕ_i vanish on $\mathbf{E}$ is*

$$\sum_{k=0}^{n-b} (-1)^k \binom{n}{k} \begin{bmatrix} n-k \\ b \end{bmatrix} . \tag{4.1}$$

Proof. For a fixed choice of $\mathbf{E}$, the number of bases of $\mathbf{V}^*$ which contain no elements of $\mathbf{E}^\perp$ is $A(n, n-b)$ as given by Proposition 4.1. The number of b-dimensional subspaces of $\mathbf{V}$ is $\begin{bmatrix} n \\ b \end{bmatrix}$, by Proposition 3.4. Therefore the number of pairs consisting of a basis and a subspace is $\begin{bmatrix} n \\ b \end{bmatrix} A(n, n-b)$. Since there are $p^{n(n-1)/2} P(n)/n!$ bases of $\mathbf{V}^*$, by Proposition 3.3d, the number of subspaces for each basis is

$$n! \begin{bmatrix} n \\ b \end{bmatrix} A(n, n-b) / (p^{n(n-1)/2} P(n)) .$$

After some simplification, we are left with equation (4.1). □

In Table 1, we give the number of uniform subspaces of small dimensions for a few sizes of affine square.

Table 1. Numbers of Uniform Subspaces

vector space	square	1	2	3	4
$\mathbf{F}_2^4$	4×4	1	13	11	1
$\mathbf{F}_2^6$	8×8	1	121	670	480
$\mathbf{F}_2^8$	16×16	1	1093	34041	122861
$\mathbf{F}_3^2$	3×3	2	1		
$\mathbf{F}_3^2$	9×9	8	84	36	1

5. The number of weakly uniform affine squares

The technique of Proposition 4.1 can be extended.

Proposition 5.1. *Let $\mathbf{V}$ be a vector space of dimension n over $\mathbf{F}_p$. Let $\mathbf{U}$ and $\mathbf{W}$ be two subspaces of $\mathbf{V}$, of dimension b and c respectively, such that $\mathbf{U} \cap \mathbf{W} = \{0\}$. Then the number of bases of $\mathbf{V}$ which contain no elements of either $\mathbf{U}$ or $\mathbf{W}$ is*

$$B_w(n, b, c) = \sum_{i=0}^{b} \sum_{j=0}^{c} \frac{(-1)^{i+j} F(b, 0, i) F(c, 0, j) B(n, i+j)}{i! j!} . \tag{5.1}$$

Proof. As in Proposition 4.1, it is sufficient to compute $W_k(\mathbf{U}\cup\mathbf{W})$. Now a linearly independent set of k elements of $\mathbf{U}\cup\mathbf{W}$ consists of i elements of $\mathbf{U}$ and j elements of $\mathbf{W}$, where $i+j=k$. Therefore

$$W_k(\mathbf{U}\cup\mathbf{W}) = \sum_{i+j=k} W_i(\mathbf{U})W_i(\mathbf{W}) \ . \tag{5.2}$$

In proving Proposition 4.1, we found an expression for $W_i(\mathbf{U})$ or $W_i(\mathbf{W})$; we substitute this in (5.2) and then apply (3.8), and (5.2) results after some simplification. □

Proposition 5.2. *The number of weakly uniform affine squares of order p^m is*

$$M_w(m) = (2m)!p^{2m}B_w(2m,m,m) \ . \tag{5.3}$$

Proof. Proposition 3.1 applies here; Φ is the set of bases which do not contain any elements of $\mathbf{E}_R^\perp \cup \mathbf{E}_C^\perp$. Therefore $|\Phi|$ is given by equation (5.1). □

6. The number of strongly uniform affine squares

The problem of counting the strongly uniform affine squares has an added complexity. We say that several vector subspaces $\mathbf{E}_1, \ldots, \mathbf{E}_n$ of a vector space $\mathbf{V}$ are **independent** if, for $\mathsf{e}_i \in \mathbf{E}_i$, the relation $\mathbf{e}_1+\cdots+\mathsf{e}_n = 0$ implies $\mathsf{e}_1 = \cdots = \mathsf{e}_n = 0$. Because $\mathbf{E}_R^\perp$ and $\mathbf{E}_C^\perp$ are independent, a subset T of $\mathbf{E}_R^\perp \cup \mathbf{E}_C^\perp$ is linearly independent if and only if each of the sets $T\cap\mathbf{E}_R^\perp$ and $T\cap\mathbf{E}_C^\perp$ is linearly independent by itself. But $\mathbf{E}_R^\perp$, $\mathbf{E}_C^\perp$, $\mathbf{E}_+^\perp$, and $\mathbf{E}_-^\perp$ are not independent. Thus there is no straightforward extension of equation (5.2).

We need some notation We let $\mathbf{V} = (\mathbf{F}_p^{2m})^*$, and if X is any of the symbols R, C, $+$, or $-$, we let

$$\begin{aligned} \mathbf{U}_X &= \mathbf{E}_X^\perp \ , \\ T_X &= T\cap\mathbf{U}_X \ , \\ a_X &= |T_X| = \dim \mathbf{V}_X \ , \end{aligned}$$

where $\mathbf{V}_X$ is the subspace of $\mathbf{V}$ spanned by T_X.

We regard $\mathbf{F}_p^{2m}$ as a direct sum of two copies of $\mathbf{F}_p^m$, so that $\mathbf{E}_R = \{(\mathsf{x},0)\,|\,\mathsf{x}\in\mathbf{F}_p^m\}$ and $\mathbf{E}_C = \{(0,\mathsf{x})\,|\,\mathsf{x}\in\mathbf{F}_p^m\}$. We also regard $\mathbf{V}$ as the direct sum of two copies of $\mathbf{W} = (\mathbf{F}_p^m)^*$. Then

$$\begin{aligned} \mathbf{U}_R &= \{(0,\mathsf{w})\,|\,\mathsf{w}\in\mathbf{W}\} \ , \\ \mathbf{U}_C &= \{(\mathsf{w},0)\,|\,\mathsf{w}\in\mathbf{W}\} \ , \\ \mathbf{U}_+ &= \{(\mathsf{w},-\mathsf{w})\,|\,\mathsf{w}\in\mathbf{W}\} \ , \text{ and} \\ \mathbf{U}_- &= \{(\mathsf{w},\mathsf{w})\,|\,\mathsf{w}\in\mathbf{W}\} \ . \end{aligned}$$

For each instance of X, we define an isomorphism j_X of $\mathbf{W}$ with $\mathbf{U}_X$ as follows:

$$j_R\mathsf{w} = (0,\mathsf{w}) \ , \tag{6.1a}$$

$$j_C\mathsf{w} = (\mathsf{w},0) \ , \tag{6.1b}$$

$$j_+\mathsf{w} = (\mathsf{w},-\mathsf{w}) \ , \text{ and} \tag{6.1c}$$

$$j_-\mathsf{w} = (0,\mathsf{w}) \ , \quad \mathsf{w}\in\mathbf{W} \ . \tag{6.1d}$$

Finally, we let

$$\mathbf{A}_X = j_X^{-1}\mathbf{V}_X \ .$$

Let us now consider the enumeration of affine squares which are uniform for $\mathbf{E}_R$, $\mathbf{E}_C$, and $\mathbf{E}_+$. These may be called **semi-strongly uniform affine squares**; of course, if $p = 2$ then "semi-strong" is equivalent to "strong." For this problem, we let $S = \mathbf{U}_R \cup \mathbf{U}_C \cup \mathbf{U}_+$, and let $\Sigma(S)$ be the simplicial complex of linearly independent subsets of S. We need to count the elements T of $\Sigma(S)$ such that $|T| = k$. Here is the plan. Each such set T determines a triple of subspaces, $(\mathbf{V}_R, \mathbf{V}_C, \mathbf{V}_+)$, which are independent. The number of sets T for a given triple depends on the dimensions of the subspaces, so we want to count the triples with given dimensions. The property of independence for such a triple is more easily examined in terms of the triple $(\mathbf{A}_R\,, \mathbf{A}_C\,, \mathbf{A}_+)$.

Proposition 6.1. *Let $\mathbf{A}_R\,$, $\mathbf{A}_C\,$, and $\mathbf{A}_+$ be subspaces of $\mathbf{W}$. Then $j_R\mathbf{A}_R\,$, $j_C\mathbf{A}_C\,$, and $j_+\mathbf{A}_+$ are independent if and only if*

$$\mathbf{A}_R \cap \mathbf{A}_C \cap \mathbf{A}_+ = \{0\}\ .$$

Proof. From (6.1a)-(6.1c) we see that $j_R\mathsf{a}_R + j_C\mathsf{a}_C + j_+\mathsf{a}_+ = 0$ if and only if $\mathsf{a}_R = \mathsf{a}_+ = -\mathsf{a}_C$. □

Proposition 6.2. *Suppose $0 \le b < m$, $a_R \ge b$, $a_C \ge b$, $a_R + a_C \le m + b$, and $a_+ \le m - b$. Then the number of triples of subspaces $(\mathbf{A}_R\,, \mathbf{A}_C\,, \mathbf{A}_+)$ such that $\dim(\mathbf{A}_R \cap \mathbf{A}_C) = b$ and $\mathbf{A}_R \cap \mathbf{A}_C \cap \mathbf{A}_+ = \{\mathsf{0}\}$ is*

$$C(a_R\,,\, a_C\,,\, b,\, a_+) = \begin{bmatrix} m \\ b \end{bmatrix} v(m,\, b,\, a_+) w(m,\, b,\, a_R\,,\, a_C)\ . \tag{6.2}$$

Proof. Let $\mathbf{B}$ denote $\mathbf{A}_R \cap \mathbf{A}_C$. The number of possibilities for $\mathbf{B}$ is $\begin{bmatrix} m \\ b \end{bmatrix}$, by Proposition 3.4. For each choice of $\mathbf{B}$, the number of possible subspaces $\mathbf{A}_+$ is given by Proposition 3.6, and the number of pairs $\{\mathbf{A}_R\,, \mathbf{A}_C\}$ is given by Proposition 3.8. □

Proposition 6.3. *The number of bases of $\mathbf{V}$ which contain no element of $\mathbf{U}_R \cup \mathbf{U}_C \cup \mathbf{U}_+$ is*

$$\begin{aligned} B_{ss}(m) = \sum_{b=0}^{m} \sum_{a_+=0}^{m-b} \sum_{a_R=b}^{m} \sum_{a_C=b}^{m+b-a_R} (-1)^{a_R+a_C+a_+} C(a_R\,,\, a_C\,,\, b,\, a_+) \cdot \\ B(a_+\,,\, 0) B(a_R\,,\, 0) B(a_C\,,\, 0) B(2m,\, a_R + a_C + a_+)\ . \end{aligned} \tag{6.3}$$

The number of semi-strongly uniform affine squares over $\mathbf{F}_p^{2m}$ is

$$M_{ss}(m) = (2m)! p^{2m} B_{ss}(m)\ . \tag{6.4}$$

Proof. Like Proposition 5.1, this follows from Theorem 3.9. The contribution to $W_k(\mathbf{U}_R \cup \mathbf{U}_C \cup \mathbf{U}_+)$ of a given selection of vector spaces $(\mathbf{A}_R\,, \mathbf{A}_C\,, \mathbf{A}_+)$ is

$$B(a_+\,,\, 0) B(a_R\,,\, 0) B(a_C\,,\, 0) B(2m,\, a_R + a_C + a_+)\ ;$$

the first three factors are the numbers of unordered bases in the respective subspaces, and the last is the number of ways of extending the union of three such bases to a basis of $\mathbf{V}$. For a given choice of $a_R\,$, $a_C\,$, a_+ , and b, where $k = a_R + a_C + a_+$, the number of triples of subspaces is found in Proposition 6.2. Finally, equation (6.4) follows as a corollary of Proposition 3.1. □

Let us now consider the enumeration of strongly uniform affine squares, for odd values of p. Our method will be similar to that which led up to Proposition 6.3; that is, we shall count linearly independent sets T by counting independent systems of subspaces $\mathbf{V}_X$. The simplicial complex for this problem is $\Sigma(S)$ where $S = \mathbf{U}_R \cup \mathbf{U}_C \cup \mathbf{U}_+ \cup \mathbf{U}_-$. The details are affected by the relation among the subspaces $\mathbf{U}_X$. We need some analogue of Proposition 6.1.

Definition 6.4. Let $\mathbf{E}$ be a vector space, with subspaces $\mathbf{A}$ and $\mathbf{B}$. Let $\mathbf{M} = \mathbf{A}+\mathbf{B}$ and $\mathbf{L} = \mathbf{A} \cap \mathbf{B}$. Then the **reversal map** determined by the pair $(\mathbf{A}, \mathbf{B})$ is the linear transformation ρ of $\mathbf{M}/\mathbf{L}$ into itself determined by

$$\rho(\mathsf{x}) = \mathsf{x} \text{ if } \mathsf{x} \in \mathbf{A}/\mathbf{L} \, ;$$
$$\rho(\mathsf{x}) = -\mathsf{x} \text{ if } \mathsf{x} \in \mathbf{B}/\mathbf{L} \, .$$

Proposition 6.5. *Let $\mathbf{V} = (\mathbf{F}_p^{2m})^*$ and $\mathbf{W} = (\mathbf{F}_p^m)^*$; if X is one of the symbols R, C, $+$, or $-$, let $\mathbf{A}_X$ be a subspace of $\mathbf{W}$, and let j_X be as in* (6.1). *Then $j_R\mathbf{A}_R$, $j_C\mathbf{A}_C$, $j_+\mathbf{A}_+$, and $j_-\mathbf{A}_-$ are independent if and only if these conditions are satisfied:*

(a) $\mathbf{A}_R \cap \mathbf{A}_+ \cap \mathbf{A}_- = 0$;
(b) $\mathbf{A}_C \cap \mathbf{A}_+ \cap \mathbf{A}_- = 0$;
(c) *if $\mathbf{M} = \mathbf{A}_+ + \mathbf{A}_-$, $\mathbf{L} = \mathbf{A}_+ \cap \mathbf{A}_-$, β is the natural map of $\mathbf{M}$ onto $\mathbf{M}/\mathbf{L}$, and ρ is the reversal map of $(\mathbf{A}_+ , \mathbf{A}_-)$, then*

$$\beta(\mathbf{A}_R \cap \mathbf{M}) \ \cap \ \rho\beta(\mathbf{A}_C \cap \mathbf{A}) = \{\mathsf{0}\} \, .$$

Proof. First, suppose these three conditions are satisfied. Let $\mathsf{a}_X \in \mathbf{A}_X$ be such that $j_R\mathsf{a}_R + j_C\mathsf{a}_C + j_+\mathsf{a}_+ + j_-\mathsf{a}_- = 0$. From equations (6.1) we see that this condition is equivalent to the two equations $\mathsf{a}_R = \mathsf{a}_+ - \mathsf{a}_-$ and $\mathsf{a}_C = -\mathsf{a}_+ - \mathsf{a}_-$. With the notation of condition (c), these equations imply that $\rho\beta\mathsf{a}_R = \beta\mathsf{a}_C$. Condition (c) therefore implies $\beta\mathsf{a}_R = \beta\mathsf{a}_C = 0$, that is, $\mathsf{a}_R \, , \, \mathsf{a}_C \in \mathbf{L}$. But then conditions (a) and (b) imply $\mathsf{a}_R = \mathsf{a}_C = 0$, and so also $\mathsf{a}_+ = \mathsf{a}_- = 0$. Thus the four spaces are independent.

Conversely, suppose the spaces $j_X\mathbf{A}_X$ are independent. Then conditions (a) and (b) follow as in Proposition 6.1. Suppose that

$$\mathsf{x} \in \beta(\mathbf{A}_R \cap \mathbf{M}) \, , \tag{6.5a}$$
$$\rho\mathsf{x} \in \beta(\mathbf{A}_C \cap \mathbf{M}) \, . \tag{6.5b}$$

Then $\mathsf{x} = \beta\mathsf{a}_R$ where $\mathsf{a}_R = \mathsf{a}_+ + \mathsf{a}_-$. By the definition of ρ, we have $\rho\mathsf{x} = \beta(-\mathsf{a}_+ + \mathsf{a}_-)$, and by (6.5b) we have $\rho\mathsf{x} = \beta\mathsf{a}_C$ for some $\mathsf{a}_C \in \mathbf{A}_C$. Therefore $\mathsf{a}_C = -\mathsf{a}_+ + \mathsf{a}_- + \mathsf{b}_\pm$, where $\mathsf{b}_\pm \in \mathbf{A}_+ \cap \mathbf{A}_-$. With these relations and equations (6.1), we find

$$j_+(2\mathsf{a}_+ - \mathsf{b}_\pm) + j_-(-2\mathsf{a}_- - \mathsf{b}_\pm) + 2j_R\mathsf{a}_R + 2j_C\mathsf{a}_C = 0 \, .$$

The assumption that the four spaces $j_X\mathbf{A}_X$ are independent now implies $\mathsf{a}_R = \mathsf{a}_C = 0$, and hence $\mathsf{x} = 0$. That is, condition (c) holds, q.e.d. □

Proposition 6.6. *Suppose that*

$$0 \le u, \quad u \le a_+ \le m, \quad \text{and } u \le a_- \le m - a_+ + u \, . \tag{6.6}$$

Then the number of pairs of subspaces $\mathbf{A}_+$ and $\mathbf{A}_-$ of $\mathbf{W}$ such that

$$\dim \mathbf{A}_+ = a_+ \, , \quad \dim \mathbf{A}_- = a_- \, , \quad \text{and } \dim(\mathbf{A}_+ \cap \mathbf{A}_-) = u \tag{6.7}$$

is

$$E_0(a_+\,,\,a_-\,,\,u) = \begin{bmatrix} m \\ u \end{bmatrix} w(m,\,u,\,a_+\,,\,a_-)\,. \tag{6.8}$$

Proof. The first factor on the right of equation (6.8) is the number of possible choices of $\mathbf{L} = \mathbf{A}_- \cap \mathbf{A}_+$. The next factor, according to Proposition 3.8, is the number of choices of $\mathbf{A}_+$ and $\mathbf{A}_+$ which intersect in a given space $\mathbf{L}$. □

Proposition 6.7. *Let $\mathbf{A}_+$ and $\mathbf{A}_-$ be subspaces of $\mathbf{W}$ such that* (6.7) *is satisfied. Let $\mathbf{M} = \mathbf{A}_+ + \mathbf{A}_-$ and $\mathbf{L} = \mathbf{A}_+ \cap \mathbf{A}_-$. Suppose that the integers b_R, b_C, a_R, and a_C satisfy*

$$0 \le b_R\,, \quad 0 \le b_C\,, \quad b_R + b_C \le a_+ + a_- - 2u\,, \tag{6.9a}$$

$$b_R \le a_R \le m + b_R - a_+ - a_- + u, \text{ and} \tag{6.9b}$$

$$b_C \le a_C \le m + b_C - a_+ - a_- + u\,. \tag{6.9c}$$

Then the number of pairs $(\mathbf{A}_R\,,\,\mathbf{A}_C)$ of subspaces of $\mathbf{W}$ such that

$$\dim \mathbf{A}_R = a_R\,, \qquad \dim(\mathbf{A}_R \cap \mathbf{M}) = b_R\,, \tag{6.10}$$

$$\dim \mathbf{A}_C = a_C\,, \qquad \dim(\mathbf{A}_C \cap \mathbf{M}) = b_C\,, \tag{6.11}$$

and the four spaces $j_X \mathbf{A}_X$ are independent is

$$\begin{aligned} E_1(a_+\,,\,a_-\,,\,u;\,b_R\,,\,b_C\,;\,a_R\,,\,a_C) = {} & \\ & w(a_+ + a_- - 2u\,,\,0,\,b_R\,,\,b_C)\cdot \\ & p^{u(b_R+b_C)} v(m - b_R\,,\,a_+ + a_- - u - b_R\,,\,a_R - b_R)\cdot \\ & \qquad v(m - b_C\,,\,a_+ + a_- - u - b_C\,,\,a_C - b_C)\,. \end{aligned} \tag{6.12}$$

Proof. The space $\mathbf{M}$ has dimension $a_+ + a_- - u$, and $\mathbf{M}/\mathbf{L}$ has dimension $a_+ + a_- - 2u$. Now $\mathbf{A}_R \cap \mathbf{M}$ has zero intersection with $\mathbf{L}$, and so $\beta(\mathbf{A}_R \cap \mathbf{M})$ has dimension b_R; similarly for $\beta(\mathbf{A}_C \cap \mathbf{M})$. This the first three inequalities of (6.9) are necessary and sufficient for b_R and b_C to be the dimensions of two independent subspaces of $\mathbf{M}/\mathbf{L}$. The inequalities relating a_R and b_R follow from $\mathbf{A}_R \cap \mathbf{M} \subseteq \mathbf{A}_R$ and $\mathbf{A}_R + \mathbf{M} \subseteq \mathbf{W}$; similarly for the inequalities relating a_C and b_C. By Proposition 3.8, the choice of the two independent spaces $\beta(\mathbf{A}_R \cap \mathbf{M})$ and $\rho\beta(\mathbf{A}_C \cap \mathbf{M})$ then accounts for the first factor in (6.12). By Proposition 3.5, the power of p represents the number of spaces $\mathbf{A}_R \cap \mathbf{M}$ for a given choice of $\beta(\mathbf{A}_R \cap \mathbf{M})$, and similarly for $\mathbf{A}_C$. The number of possibilities for $\mathbf{A}_R$, given its intersection with $\mathbf{M}$, is shown by Proposition 3.7 to be the next factor, and the last one corresponds similarly to $\mathbf{A}_C$. □

Proposition 6.8. *Let the notations T, $\mathbf{U}_X$, $\mathbf{V}_X$, $\mathbf{A}_X$, j_X, and a_X be as given near the beginning of this section. Suppose that u, a_+, and a_- satisfy* (6.6). *Suppose furthermore that b_R, b_C, a_R, and a_C satisfy* (6.7) *and* (6.9). *Then the number of liearly independent subsets T of $\mathbf{U}_R \cup \mathbf{U}_C \cup \mathbf{U}_+ \cup \mathbf{U}_-$ such that $\dim(\mathbf{A}_+ \cap \mathbf{A}_-) = u$, $\dim(\mathbf{A}_R \cap (\mathbf{A}_+ + \mathbf{A}_-)) = b_R$, and $\dim(\mathbf{A}_C \cap (\mathbf{A}_+ + \mathbf{A}_-)) = b_C$ is*

$$\begin{aligned} E(a_+\,,\,a_-\,,\,u\,;\,b_R\,,\,b_C\,;\,a_R\,,\,a_C) = {} & \\ & E_0(a_+\,,\,a_-\,,\,u)\cdot \\ & E_1(a_+\,,\,a_-\,,\,u\,;\,b_R\,,\,b_C\,;\,a_R\,,\,a_C)\cdot \\ & \qquad B(a_R\,,\,0)B(a_C\,,\,0)B(a_+\,,\,0)B(a_-\,,\,0)\,. \end{aligned} \tag{6.13}$$

Proof. The factor E_0 is the number of ways to choose $\mathbf{A}_+$ and $\mathbf{A}_-$, according to Proposition 6.6. Proposition 6.7 then gives the factor E_1 as the number of ways to choose $\mathbf{A}_R$ and $\mathbf{A}_C$. Finally, the last four factors are the numbers of bases of the respective vector spaces. □

Proposition 6.9. *The number of bases of* $\mathbf{V}$ *which contain no element of* $\mathbf{U}_R \cup \mathbf{U}_C \cup \mathbf{U}_+ \cup \mathbf{U}_-$ *is*

$$B_s(m) = \sum_{u=0}^{m} \sum_{a_+=u}^{m} \sum_{a_-=u}^{m} \sum_{b_R=0}^{a_+ + a_- - 2u} \Bigg(\sum_{b_C=0}^{(a_+ + a_- - 2u - b_R)} \sum_{a_R=b_R}^{(m + b_R - a_+ - a_- + u)} \sum_{a_C=b_C}^{(m + b_C - a_+ - a_- + u)} \Bigg((-1)^{a_R + a_C + a_+ + a_-} E(a_+\,,\, a_-\,,\, u\,;\, b_R\,,\, b_C\,;\, a_R\,,\, a_C) \cdot B(2m, a_R + a_C + a_+ + a_-) \Bigg) \Bigg) \,. \tag{6.14}$$

The number of strongly affine magic squares over $\mathbf{F}_p^{2m}$ *is*

$$M_s(m) = (2m)! p^{2m} B_s(m) \,. \tag{6.15}$$

Proof. As for Proposition 6.2. □

Table 2 gives some values of the numbers we have described.

TABLE 2. Numbers of Bases Satisfying different conditions

$\mathbf{F}_p^{2m}$	square	$A(2m,m)$	$B_w(2m,m,m)$	$B_{ss}(m)$
$\mathbf{F}_2^4$	4×4	312	81	9
$\mathbf{F}_2^6$	8×8	13,447,168	5,821,200	2,192,904
$\mathbf{F}_2^8$	16×16	81,162,330,439,680	48,087,051,969,600	27,461,244,928,320
$\mathbf{F}_3^2$	3×3	12	4	0
$\mathbf{F}_3^4$	9×9	653,184	399,744	228,096
$\mathbf{F}_3^6$	27×27	93,808,434,769,920	74,685,971,483,136	58,927,823,046,144
$\mathbf{F}_5^2$	5×5	160	96	48
$\mathbf{F}_5^4$	25×25	4,128,000,000	3,500,697,600	2,947,718,400

$\mathbf{F}_p^{2m}$	square	$B_s(m)$
$\mathbf{F}_3^2$	3×3	0
$\mathbf{F}_3^4$	9×9	118,656
$\mathbf{F}_3^6$	27×27	46,042,984,825,344
$\mathbf{F}_5^2$	5×5	16
$\mathbf{F}_5^4$	25×25	2,462,956,800

7. The number of affine magic squares of odd order

We turn now to the most difficult of our problems. We solve it in several steps. First, we count the affine magic squares determined by a basis of $\mathbf{V}$ satisfying certain conditions; then we apply the general Möbius inversion formula to determine the number of such bases. As in the latter part of §5, the simplicial complex is $\Sigma(S)$ where $S = \mathbf{U}_R \cup \mathbf{U}_C \cup \mathbf{U}_+ \cup \mathbf{U}_-$. This leaves us with another problem of counting linearly independent sets of vectors; as before, we solve this problem by relating the vectors to certain vector subspaces.

From Proposition 2.10, we know that an affine magic square is weakly uniform; that is, the linear parts of its digit coordinates do not belong to $\mathbf{U}_R \cup \mathbf{U}_C$. However, some of them may belong to $\mathbf{U}_+ \cup \mathbf{U}_-$, as we see from Proposition 2.12.

Proposition 7.1. *Let Φ be a basis of $(\mathbf{F}_p^{2m})^*$, containing no elements of $\mathbf{U}_R \cup \mathbf{U}_C$ and b elements of $\mathbf{U}_+ \cup \mathbf{U}_-$. Then there are $(2m)!p^{2m-b}$ affine magic squares $\mathbf{S}$ such that $\Phi = \{A_1^L, \ldots, A_{2m}^L\}$ where the A_j are the digit coordinates of $\mathbf{S}$.*

Proof. The digit coordinates of $\mathbf{S}$ may be taken in any order to give a different magic square; this fact accounts for the factor $(2m)!$. In the notation of Proposition 2.12, $J_+ \cup J_-$ contains b elements; for each of these, A_j is determined uniquely by A_j^L and the requirement that $A_j(\mathsf{x}_0) = (p-1)/2$. For the other $2m-b$ digit coordinates, $A_j(\mathsf{x}_0)$ is unrestricted; this fact accounts for the factor p^{2m-b}. □

Proposition 7.2. *If J_+ and J_- are linearly independent subsets of $\mathbf{U}_+$ and $\mathbf{U}_-$ respectively, let $P(J_+, J_-, w)$ be the number of linearly independent sets of vectors T such that $|T| = w$ and*

$$J_+ \cup J_- \subseteq T \subseteq S .$$

Then the number of affine magic squares of odd order p^m is

(7.1)

$$M(m) = \sum_{J_+, J_-} (2m)!p^{2m-|J_+|-|J_-|} \sum_w (-1)^{w-|J_+|-|J_-|} P(J_+, J_-, w) B(2m, w) .$$

Proof. For each $\alpha \in \Sigma(S)$ let $g(\alpha)$ be the number of bases B of $\mathbf{V}$ such that $B \cap S \supseteq \alpha$, and let $f(\beta)$ be the number of bases B of $\mathbf{V}$ such that $B \cap S = \beta$. Then

$$g(\alpha) = \sum_{\substack{\beta \in \Sigma(S) \\ \beta \supseteq \alpha}} f(\beta) ,$$

so by the Möbius inversion formula [9]

$$f(\beta) = \sum_{\substack{\alpha \in \Sigma(S) \\ \alpha \supseteq \beta}} \mu(\beta, \alpha) g(\alpha) .$$

But $\mu(\beta, \alpha) = (-1)^{(|\alpha|-|\beta|)}$, and $g(\alpha) = B(2m, |\alpha|)$; and the number of terms in the preceding sum, for $\beta = J_+ \cup J_-$, is $P(J_+, J_-, |\alpha|)$. We therefore have

$$f(J_+ \cup J_-) = \sum_w (-1)^{w-|J_+|-|J_-|} P(J_+, J_-, w) B(2m, w) ;$$

and the desired expression for $M(m)$ now follows from Proposition 7.1. □

We now face the problem of evaluating $P(J_+\,,\,J_-\,,\,w)$. This is like the problem which we solved in Proposition 6.8. We recall some more of the notation used in §6; in particular, if X is any one of the symbols R, C, $+$, or $-$, we recall $\mathbf{V}_X$, j_X, and $\mathbf{A}_X$. We also define subspaces $\mathbf{B}_+$ and $\mathbf{B}_-$ of $\mathbf{W}$ so that $j_+\mathsf{B}_+$ is the subspace spanned by J_+, and similarly for $\mathbf{B}_-$. The problem of counting sets T will be reduced to that of counting quadruples $(\mathbf{A}_R\,,\,\mathbf{A}_C\,,\,\mathbf{A}_+\,,\,\mathbf{A}_-)$ such that $j_R\mathbf{A}_R$, $j_C\mathbf{A}_C$, $j_+\mathbf{A}_+$, and $j_-\mathbf{A}_-$ are linearly independent and also

$$\mathbf{A}_+ \supseteq \mathbf{B}_+\,, \tag{7.2}$$

$$\mathbf{A}_- \supseteq \mathbf{B}_-\,. \tag{7.3}$$

We begin by counting the choices of $(\mathbf{A}_+\,,\,\mathbf{A}_-)$, subject to the constraint of equations (7.2). We have to keep several subspaces of $\mathbf{W}$ in mind. To organize the details, we must consider the lattice of subspaces of $\mathbf{W}$.

The classic reference on lattices is [3]. The vector subspaces of a vector space are a lattice, in which the elements are partially ordered by containment, the "meet" operation is intersection, and the "join" operation is the sum. It is a "modular" lattice; that is, if $\mathbf{X} \subseteq \mathbf{Z}$ then

$$\mathbf{X} + (\mathbf{Y} \cap \mathbf{Z}) = (\mathbf{X} + \mathbf{Y}) \cap \mathbf{Z}\,.$$

We deal with the sublattice generated by $(\mathbf{A}_R\,,\,\mathbf{A}_C\,,\,\mathbf{A}_+\,,\,\mathbf{A}_-)$; the generators satisfy (7.2). Without making any other assumptions about these four subspaces, we are looking at an example of the solved problem of a "Free modular lattice generated by two chains" ([3], §7). Even without the general theory, it is not hard to verify that in general the lattice generated by our four subspaces is as in Figure 1.

In this figure, each line segment connects a vector space with a subspace; we may associate the difference in their dimensions with the segment. For every parallelogram in the figure, the well-known formula

$$\dim(\mathbf{E} + \mathbf{F}) + \dim(\mathbf{E} \cap \mathbf{F}) = \dim(\mathbf{E}) + \dim(\mathbf{F})$$

relates the dimensions of the spaces named at the four vertices, and implies that the numbers associated with opposite sides of the parallelogram are equal. Thus the dimensions of the vector spaces are determined by the following nine non-negative integers:

$$b_0 = \dim(\mathbf{B}_+ \cap \mathbf{B}_-)\,; \tag{7.4a}$$

$$\rho_+ = \dim(\mathbf{A}_- \cap \mathbf{B}_+) - \dim(\mathbf{B}_- \cap \mathbf{B}_+)\,; \tag{7.4b}$$

$$\rho_- = \dim(\mathbf{A}_+ \cap \mathbf{B}_-) - \dim(\mathbf{B}_+ \cap \mathbf{B}_-)\,; \tag{7.4c}$$

$$\sigma_+ = \dim(\mathbf{B}_+) - \dim(\mathbf{A}_- \cap \mathbf{B}_+)\,; \tag{7.4d}$$

$$\sigma_- = \dim(\mathbf{B}_-) - \dim(\mathbf{A}_+ \cap \mathbf{B}_1)\,; \tag{7.4e}$$

$$\phi = \dim \mathbf{L} - \dim(\mathbf{L} \cap \mathbf{B})\,; \tag{7.4f}$$

$$\tau_+ = \dim(\mathbf{A}_+) - \dim(\mathbf{L} + \mathbf{B}_+)\,; \tag{7.4g}$$

$$\tau_- = \dim(\mathbf{A}_-) - \dim(\mathbf{L} + \mathbf{B}_-)\,; \tag{7.4h}$$

$$\psi = m - \dim(\mathbf{M})\,; \tag{7.4i}$$

which satisfy

$$m = b_0 + \rho_+ + \rho_- + \sigma_+ + \sigma_- + \phi + \tau_+ + \tau_- + \psi\,. \tag{7.5}$$

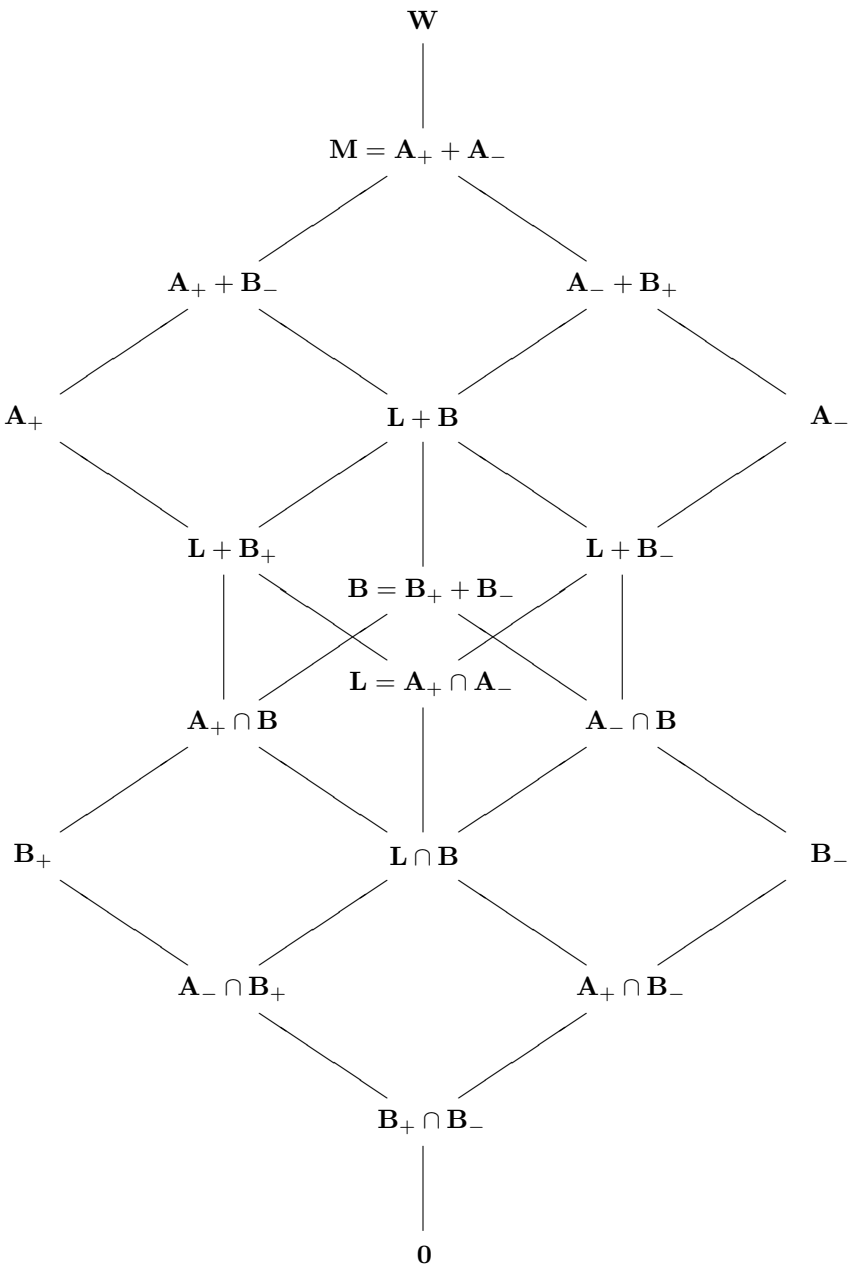

FIGURE 1. The lattices of subspaces generated by $(\mathbf{A}_R\,,\,\mathbf{A}_C\,,\,\mathbf{A}_+\,,\,\mathbf{A}_-)$

Specifically, we have

$$
\begin{aligned}
&(7.6a) && e_+ = \dim(\mathbf{A}_- \cap \mathbf{B}_+) && = b_0 + \rho_+ \, ; \\
&(7.6b) && e_- = \dim(\mathbf{A}_+ \cap \mathbf{B}_-) && = b_0 + \rho_- \, ; \\
&(7.6c) && b_+ = \dim(\mathbf{B}_+) && = b_0 + \rho_+ + \sigma_+ \, ; \\
&(7.6d) && b_- = \dim(\mathbf{B}_-) && = b_0 + \rho_- + \sigma_- \, ; \\
&(7.6e) && u = \dim(\mathbf{A}_+ \cap \mathbf{A}_-) && = b_0 + \rho_+ + \rho_- + \phi \, ; \\
&(7.6f) && a_+ = dim(\mathbf{A}_+) && = b_0 + \rho_+ + \rho_- + \sigma_+ + \phi + \tau_+ \, ; \\
&(7.6g) && a_- = dim(\mathbf{A}_+) && = b_0 + \rho_+ + \rho_- + \sigma_- + \phi + \tau_- \, .
\end{aligned}
$$

We shall let $\mathbf{x}$ stand for an element $(b_0 \, ; \, \rho_+ \, , \, \rho_- \, ; \, \sigma_+ \, , \, \sigma_- \, ; \, \tau_+ \, , \, \tau_- \, ; \, \phi, \psi) \in \mathbb{N}^9$, and let $\mathbf{T}(m)$ be the set of all such $\mathbf{x}$ subject to the constraint (7.5).

Proposition 7.3. *Let $\mathbf{x} \in \mathbf{T}(m)$. Let $\mathbf{B}_+$ and $\mathbf{B}_-$ be subspaces of $\mathbf{W}$ satisfying* (7.4a), (7.6c), *and* (7.6d). *Then the number of pairs $(\mathbf{A}_+ \, , \, \mathbf{A}_-)$ of subspaces of $\mathbf{W}$ satisfying the relations* (7.2) *and* (7.6) *is*

$$
\begin{aligned}
F_0(\mathbf{x}) = \begin{bmatrix} \sigma_+ + \rho_+ \\ \rho_+ \end{bmatrix} \begin{bmatrix} \sigma_- + \rho_- \\ \rho_- \end{bmatrix} \cdot & \\
v(m - \rho_+ - \rho_- - b_0 \, , \, \sigma_+ + \sigma_- \, , \, \phi) \cdot & \\
v(\sigma_- + \tau_+ + \tau_- + \psi, \, \sigma_- \, , \, \tau_+) \cdot & \\
v(\sigma_+ + \tau_+ + \tau_- + \psi, \, \tau_+ + \sigma_+ \, , \, \tau_-) \, . &
\end{aligned}
$$

Proof. We repeatedly apply Proposition 3.7. First, $\mathbf{A}_- \cap \mathbf{B}_+$ is an e_+-dimensional subspace $\mathbf{X}$ of $\mathbf{B}_+$, satisfying $\mathbf{X} \cap (\mathbf{B}_+ \cap \mathbf{B}_-) = (\mathbf{B}_+ \cap \mathbf{B}_-)$; the number of these is $v(b_+ - b_0 \, , \, 0, \, e_+ - b_0) = \binom{b_+ - b_0}{e_+ - b_0}$. Similarly, the second factor is the number of choices for $\mathbf{A}_+ \cap \mathbf{B}_-$. The spaces $\mathbf{A}_- \cap \mathbf{B}_+$ and $\mathbf{A}_+ \cap \mathbf{B}_-$ together determine $\mathbf{L} \cap \mathbf{B}$. The next factor is the number of choices of $\mathbf{L}$, given its intersection with $\mathbf{B}$. The choice of $\mathbf{L}$ determines $\mathbf{L} + \mathbf{B}_+$, $\mathbf{L} + \mathbf{B}$, and $\mathbf{L} + \mathbf{B}_-$. The fourth factor is the number of choices of $\mathbf{A}_+$, given that its intersection with $\mathbf{L} + \mathbf{B}$ is $\mathbf{L} + \mathbf{B}_+$. The choice of $\mathbf{A}_+$ determines $\mathbf{A}_+ + \mathbf{B}_-$. Finally, the last factor is the number of choices of $\mathbf{A}_-$ given that its interseection with $\mathbf{A}_+ + \mathbf{B}_-$ is $\mathbf{L} + \mathbf{B}_-$. □

Let us now consider the subspaces $\mathbf{A}_R$ and $\mathbf{A}_C$. They are related to $\mathbf{A}_+$ and $\mathbf{A}_-$ by (6.9) and (6.11); we see that the constraints on the dimensions of the spaces involved are equivalent to

$$
\begin{aligned}
&(7.7a) && 0 \le b_R \, , \\
&(7.7b) && 0 \le b_C \, , \\
&(7.7c) && b_R + b_C \le \sigma_+ + \sigma_- + \tau_+ + \tau_- \, , \\
&(7.7d) && b_R \le a_R \le b_R + \psi \, , \\
&(7.7e) && b_C \le a_C \le b_C + \psi \, .
\end{aligned}
$$

Let $\mathbf{U}(\mathbf{x})$ denote the set of all $\mathbf{y} = (b_R \, , \, b_C \, , \, a_R \, , \, a_C) \in \mathbb{N}^4$ subject to (7.7).

Proposition 7.4. *Let $\mathbf{x} \in \mathbf{T}(m)$ and $\mathbf{y} \in \mathbf{U}(\mathbf{x})$. Let J_+ and J_- be indepenent subsets of $\mathbf{U}_+$ and $\mathbf{U}_-$ respectively; let $\mathbf{B}_+$ and $\mathbf{B}_+$ be subspaces of $\mathbf{W}$ such that $j_+\mathbf{B}_+$ is the subspace spanned by J_+, and similarly for J_- and $\mathbf{B}_-$; let* (7.4a), (7.6c), *and* (7.6d) *be satisfied. Then the number of linearly independent subsets T*

of $\mathbf{U}_R \cup \mathbf{U}_C \cup \mathbf{U}_+ \cup \mathbf{U}_-$ *such that (a)* $T \cap \mathbf{U}_+ = J_+$ *, (b)* $T \cap \mathbf{U}_- = J_{-+}$ *and (c) the dimensions of subspaces are as given in* (7.6) *and* (7.7) *is*

$$F(\mathbf{x},\mathbf{y}) = F_0(\mathbf{x}) E_1(a_+\,,\, a_-\,,\, u;\, b_R\,,\, b_C\,;\, a_R\,,\, a_C)\cdot \\ B(a_+\,,\, b_+)B(a_-\,,\, b_-)B(a_R\,,\, 0)B(a_C\,,\, 0)\,. \tag{7.8}$$

Proof. The number of pairs $(\mathbf{A}_+\,,\, \mathbf{A}_-)$ satisfying the conditions of the proposition is the first factor on the right of (7.8), by Proposition 7.3. Given $(\mathbf{A}_+\,,\, \mathbf{A}_-)$, the number of pairs $(\mathbf{A}_R\,,\, \mathbf{A}_C)$ is the second factor, as given by Proposition 6.7. The last four factors are applications of Proposition 3.3b. □

Proposition 7.5. *The number of affine magic squares of odd order* p^m *is*

$$M(m) = \\ \sum_{\mathbf{x}\in\mathbf{T}(m)} \sum_{\mathbf{Y}\in\mathbf{U}(\mathbf{x})} (-1)^{\rho_+ + \rho_- + \tau_+ + \tau_- + a_R + a_C} (2m)! p^{2m - 2b_0 - \rho_+ - \rho_- - \sigma_+ - \sigma_-}\,. \\ F(\mathbf{x},\mathbf{y}) B(2m, a_+ + a_- + a_R + a_C) B(b_+\,,\, 0) B(b_-\,,\, 0)\cdot \\ \begin{bmatrix} m \\ b_0 \end{bmatrix} \begin{bmatrix} m - b_0 \\ b_+ - b_0 \end{bmatrix} v(m - b_0\,,\, b_+ - b_0\,,\, b_- - b_0)\,. \tag{7.9}$$

Here the notation of (7.6) *is used.*

Proof. This follows from Proposition 7.2. The summation over J_+ and J_- in (7.1) can be arranged as a summation over the choices of vector spaces $\mathbf{B}_+$ and $\mathbf{B}_-$, followed by a summation, for fixed $\mathbf{B}_+$ and $\mathbf{B}_-$, over the different bases of these spaces. The number of such bases accounts for the factors $B(b_+\,,\, 0)$ and $B(b_-\,,\, 0)$ in (7.5). The summation over choices of $\mathbf{B}_+$ and $\mathbf{B}_-$ may be organized as a summation over the dimensions of these spaces and of their intersection, followed by a summation over the set of possible spaces, for fixed values of these dimensions. The number of choices of the intersection, then of $\mathbf{B}_+$, and then of $\mathbf{B}_-$ give the last three factors in (7.9).

From Proposition 7.4 it is clear that the quantity $P(J_+\,,\, J_-)$ defined in Proposition 7.2 is a summation of $F(\mathbf{x},\mathbf{y})$ over a suitable set of pairs $\mathbf{x},\mathbf{y})$. Specifically, if J_+ spans $j_+\mathbf{B}_+$, and J_- spans $j_-\mathbf{B}_-$, then the set is

$$\{(\mathbf{x},\mathbf{y}) \in \mathbf{T}(m) \times \mathbb{N}^4 \,|\, \mathbf{y} \in \mathbf{U}(\mathbf{x}) \text{ and} \\ b_0 = \dim(\mathbf{B}_+ \cap \mathbf{B}_-) \text{ and} \\ b_0 + \rho_+ + \sigma_+ = |J_+| \text{ and } b_0 + \rho_- + \sigma_- = |J_-| \text{ and} \\ 2b_0 + 2\rho_+ + 2\rho_- + \sigma_+ + \sigma_- + 2\phi + \tau_+ + \tau_- + a_R + a_C = w\}\,.$$

Therefore the sum over the dimensions $b_0\,,\, b_+$, and b_- together with w, in equation (7.1), reduces to the summation given in (7.9). □

Table 3 gives some values of $M(m)$. Note that we have counted as distinct two squares which differ only by a geometrical transformation such as a rotation. For this reason we also give the value of $M/8$.

References

1. Allan Adler, *Magic cubes and the 3-adic zeta function*, Math. Intelligencer **14** (1992), no. 3, 14–23.

TABLE 3. The Number of Affine Magic Squares

$\mathbf{F}_p^{2m}$	square	$M(m)$	$M(m)/8$
$\mathbf{F}_3^2$	3×3	8	1
$\mathbf{F}_3^4$	9×9	365,921,280	45,740,160
$\mathbf{F}_3^3$	27×27	28,540,989,964,033,597,440	3,567,623,745,504,199,680
$\mathbf{F}_5^2$	5×5	1,472	184
$\mathbf{F}_5^4$	25×25	39,757,569,638,400	4,969,696,204,800

2. William H. Benson and Oswald Jacoby, *New Recreations with Magic Squares*, Dover, New York, 1976.
3. Garrett Birkhoff, *Lattice Theory*, American Mathematical Society, Providence, R. I., 1984.
4. J. Goldman and G.-C. Rota, *On the foundations of combinatorial theory IV: finite vector spaces and Eulerian generating functions*, Studies in Appl. Math. **49** (1970), 239–258.
5. C. J. Henrich, *Magic squares and linear algebra*, American Math. Monthly **98** (1991), 481–488.
6. J. W. P. Hirschfeld, *Projective Geometries over Finite Fields*, Oxford University Press, Oxford, 1979.
7. S. A. Joni and G.-C. Rota, *A vector space analog of permutations with restricted position*, J. Combin. Theo, **29** (1980), 59–73.
8. Maurice Kraïtchik, *Mathematical Recreations*, 2 ed., Dover, New York, 1953.
9. G.-C. Rota, *On the foundations of combinatorial theory I. theory of Möbius functions*, Zeitsch. für Wahrscheinlichkeit u. Verw. Geb. **2** (1964), 340–368.
10. H. M. Stark, *An Introduction to Number Theory*, Markham, Chicago, 1970.
11. Eric W. Weisstein, *"q-binomial coefficient." from Mathworld – A Wolfram Web Resource.*, `http://mathworld.wolfram.com/q-BinomialCoefficient.html`.

19 TILLINGHAST PLACE, BUFFALO, NY 14216
E-mail address: `chenrich@monmouth.com`