Optimal binary constant weight codes and affine linear groups over finite fields

Xiang-Dong Hou

Abstract
The affine linear group of degree one, $\text{AGL}(1, \mathbb{F}_q)$, over the finite field $\mathbb{F}_q$, acts sharply two-transitively on $\mathbb{F}_q$. Given $S < \text{AGL}(1, \mathbb{F}_q)$ and an integer $k$, $1 \leq k \leq q$, does there exist a $k$-element subset $B \subset \mathbb{F}_q$ whose set-wise stabilizer is $S$? Our main result is the derivation of two formulas which provide an answer to this question. This result allows us to determine all possible parameters of binary constant weight codes that are constructed from the action of $\text{AGL}(1, \mathbb{F}_q)$ on $\mathbb{F}_q$ to meet the Johnson bound. Consequently, for many parameters, we are able to determine the values of the function $A_2(n, d, w)$, which is the maximum number of codewords in a binary constant weight code of length $n$, weight $w$ and minimum distance $\geq d$.

Keywords Affine linear group · BIBD · Constant weight code · Johnson bound

Mathematics Subject Classification 05B05 · 05E18 · 94B25

1 Introduction

Let $\mathbb{F}_q$ denote the finite field with $q$ elements. A binary constant weight code of length $n$ is a subset $C \subset \mathbb{F}_q^n$ such that every codeword of $C$ has the same Hamming weight. Let $n$, $d$, $w$ be positive integers. By an $(n, d, w)_2$ code, we mean a binary constant weight code of length $n$, weight $w$ and minimum distance $\geq d$. (This is not standard notation in coding theory, however, it serves our purposes conveniently.) Let $A_2(n, d, w)$ be the maximum number of codewords in an $(n, d, w)_2$ code. In [11], Johnson used bounds on $A_2(n, d, w)$ to strengthen the sphere packing bound for the minimum distance of error-correcting codes. Since then, the function $A_2(n, d, w)$ has become an important concept in coding theory, and its values have been the focus of numerous studies in coding theory and combinatorial designs; see for example [1,3,4,7,11–13,15,17,18]. A fundamental fact about the function $A_2(n, d, w)$ is the following upper bound.

Communicated by Q. Xiang.

Xiang-Dong Hou
xhou@usf.edu

1 Department of Mathematics and Statistics, University of South Florida, Tampa, FL 33620, USA
Theorem 1.1 (The restricted Johnson bound [11], [10, Sect. 2.3.1]) We have
\[
A_2(n, d, w) \leq \frac{nd}{2w^2 - 2nw + nd}
\] (1.1)
provided \(2w^2 - 2nw + nd > 0\).

When \(d = 2\delta\), (1.1) gives
\[
A_2(n, 2\delta, w) \leq \frac{n\delta}{w^2 - nw + n\delta}
\] (1.2)
provided \(w^2 - nw + n\delta > 0\). The codes achieving the equality in (1.2) are precisely those constructed from balanced incomplete block designs.

A balanced incomplete block design (BIBD) with parameters \((v, b, r, k, \lambda)\), where the parameters are positive integers, is a pair \(D = (V, B)\), where \(V = \{x_1, \ldots, x_v\}\) is a \(v\)-element set and \(B = \{B_1, \ldots, B_b\}\) is a family of \(k\)-element subsets of \(V\), called blocks, such that each element of \(V\) belongs to \(r\) blocks and any two elements of \(V\) belong to \(\lambda\) blocks. The incidence matrix of \(D\) is the \(v \times b\) matrix \(A = (a_{ij})\) where
\[
a_{ij} = \begin{cases} 
1 & \text{if } x_i \in B_j, \\
0 & \text{otherwise}.
\end{cases}
\]
The obvious relations \(bk = vr\) and \(r(k - 1) = \lambda(v - 1)\) allow \(r\) and \(b\) to be expressed in terms of \(v, k\) and \(\lambda\):
\[
r = \frac{\lambda(v - 1)}{k - 1}, \quad b = \frac{\lambda v(v - 1)}{k(k - 1)}.
\] (1.3)
Hence a \((v, b, r, k, \lambda)\) BIBD is also called a \((v, k, \lambda)\) BIBD. We treat the \((0, 1)\)-matrix \(A\) as being over \(\mathbb{F}_2\) and let \(R(A)\) denote the set of rows of \(A\). Then \(R(A)\) is an \((n, 2\delta, w)_2\) code with minimum distance \(2\delta\), where
\[
\begin{cases} 
n = b = \frac{\lambda v(v - 1)}{k(k - 1)}, \\
\delta = r - \lambda = \frac{\lambda(v - k)}{k - 1}, \\
w = r = \frac{\lambda(v - 1)}{k - 1}.
\end{cases}
\] (1.4)

Theorem 1.2 ([14], [18, Theorem 2.4.12]) An \((n, 2\delta, w)_2\) code \(C\) with \(|C| = n\delta/(w^2 - nw + n\delta)\) is precisely of the form \(C = R(D)\), where \(D\) is the incidence matrix of a \((v, b, r, k, \lambda)\) BIBD whose parameters satisfy (1.4). Hence the equality in (1.2) holds if and only if there exists a \((v, b, r, k, \lambda)\) BIBD whose parameters satisfy (1.4).

Let \(G\) be a finite group acting 2-transitively on a finite set \(V\) and let \(B \subset V\) be such that \(|B| \geq 2\). Let \(B = \{g(B) : g \in G\}\) and let
\[
G_B = \{g \in G : g(B) = B\} \leq G
\]
be the set-wise stabilizer of \( B \) in \( G \). It is obvious that \((V, B)\) is a BIBD; its parameters are given by
\[
\begin{align*}
v &= |V|, \\
b &= \frac{|G|}{|G_B|}, \\
r &= \frac{|B| |G|}{|V| |G_B|}, \\
k &= |B|, \\
\lambda &= \frac{|B|(|B| - 1) |G|}{|V|(|V| - 1)|G_B|}.
\end{align*}
\] 
(1.5)

With \( G \) and \( V \) given, the parameters of \((V, B)\) are determined by \(|B|\) and \(|G_B|\). Therefore, an answer to the following question would determine all possible parameters of \((V, B)\).

**Question 1.3** Let \( G \) be a finite group acting on a finite set \( V \). Let \( S \leq G \) and \( 0 \leq k \leq |V| \).

Does there exist \( B \subset V \) with \(|B| = k\) such that \( S = G_B \)?

For any set \( X \) and any integer \( k \geq 0 \), let \( \binom{X}{k} = \{ B \subset X : |B| = k \} \). The affine linear group \( \text{AGL}(1, \mathbb{F}_q) \) acts (sharply) two-transitively on \( \mathbb{F}_q \). Our main objective is to answer Question 1.3 for this action. More precisely, we determine all subgroups of \( \text{AGL}(1, \mathbb{F}_q) \), and for each \( S < \text{AGL}(1, \mathbb{F}_q) \) and each \( 0 \leq k \leq q \), we derive formulas that give the number of \( B \in \binom{\mathbb{F}_q}{k} \) such that \( S = \text{AGL}(1, \mathbb{F}_q)_B \). Consequently, we are able to describe the possible parameters of the BIBDs constructed from the action of \( \text{AGL}(1, \mathbb{F}_q) \) on \( \mathbb{F}_q \).

By Theorem 1.2, the corresponding values of the function \( A_2(n, 2\delta, w) \) are determined. More precisely, if there exist integers \( k \geq 2 \) and \( s > 0 \) such that there are \( S < \text{AGL}(a, \mathbb{F}_q) \) and \( B \in \binom{\mathbb{F}_q}{k} \) with \(|S| = s\) and \( S = \text{AGL}(1, \mathbb{F}_q)_B \), then there is a \((q, k, k(k - 1)/s)\) BIBD and hence
\[
A_2\left( \frac{q(q-1)}{s}, \frac{2k(k-k)}{s}, \frac{k(q-1)}{s} \right) = q.
\] 
(1.6)

Sun [16] constructed various subsets of \( \mathbb{F}_q \) and determined their stabilizers in \( \text{AGL}(1, \mathbb{F}_q) \).

The approach of the present paper is a little different; we are interested in the existence of \( B \in \binom{\mathbb{F}_q}{k} \), not its description, such that \( \text{AGL}(1, \mathbb{F}_q)_B \) is a given subgroup of \( \text{AGL}(1, \mathbb{F}_q) \).

Question 1.3, in its general form, does not seem to have appeared in the literature. However, for two special cases, \( \text{PGL}(2, \mathbb{F}_q) \) and \( \text{PSL}(2, \mathbb{F}_q) \) acting on the projective line \( \text{PG}(1, \mathbb{F}_q) \), the question has been considered by Cameron et al. [6] and by Cameron et al. [5]. The purpose there is to determine possible parameters of 3-designs admitting \( \text{PGL}(2, \mathbb{F}_q) \) or \( \text{PSL}(2, \mathbb{F}_q) \) as an automorphism group. As illustrated in [5,6], the number of subsets \( B \) in Question 1.3 can be computed from the Möbius function (of the lattice of subgroups) of \( G \). We mention that the Möbius functions of \( \text{PGL}(2, \mathbb{F}_q) \) and \( \text{PSL}(2, \mathbb{F}_q) \) have not been completely determined.

The paper is organized as follows. In Sect. 2, we describe a strategy for solving Question 1.3. Section 3 provides the necessary background on \( \text{AGL}(1, \mathbb{F}_q) \) and its subgroups. Section 4 contains the main results of the paper. Theorems 4.2 and 4.4 give formulas for the function \( N(S, k) = |\{ B \in \binom{\mathbb{F}_q}{k} : S = \text{AGL}(1, \mathbb{F}_q)_B \}| \), where \( S < \text{AGL}(1, \mathbb{F}_q) \) and \( 0 \leq k \leq q \). The input data of the aforementioned formulas are explained in Sect. 5. Section 6 contains some additional remarks about Question 1.3, where we also show that the numerical results from our formulas are consistent with the existing theoretic results. The section also includes several open questions. The appendix supplies the reader with a Mathematica code for computing the function \( N(S, k) \) and a table of values of \( N(S, k) \) with \( q \leq 16 \). (An extended table of values of \( N(S, k) \) with \( q \leq 101 \) is available in [8]).
2 A strategy for solving question 1.3

Let $G$ be a finite group acting on a finite set $V$. Let $S < G$ and $0 \leq k \leq |V|$ and define

$$S' = \left\{ B \in \binom{V}{k} : \sigma(B) = B \text{ for all } \sigma \in S \right\}.$$  \hspace{1cm} (2.1)

(We remind the reader that the operation $(\cdot)'$ depends on $k$.) Note that a subset $B$ of $V$ belongs to $S'$ if and only if $B$ is a union of $S$-orbits in $V$ with $|B| = k$. If the sizes of the $S$-orbits are known, then $|S'|$ is easily determined. Let $S_1, \ldots, S_t$ be the minimal elements of $\{ T : S \leq T < G \}$; these are the immediate supergroups of $S$ in $G$. Then by the inclusion-exclusion principle,

$$\left| \left\{ B \in \binom{V}{k} : S = GB \right\} \right| = |S'| - |S_1' \cup \cdots \cup S_t'|$$

$$= |S'| - \sum_{l=1}^{t} (-1)^{l-1} \sum_{1 \leq i_1 < \cdots < i_l \leq t} |S_1' \cap \cdots \cap S_l'|$$

$$= |S'| + \sum_{l=1}^{t} (-1)^l \sum_{1 \leq i_1 < \cdots < i_l \leq t} |(S_1' \cup \cdots \cup S_l)'|$$

$$= \sum_{l=0}^{t} (-1)^l \sum_{1 \leq i_1 < \cdots < i_l \leq t} |\langle S \cup S_1' \cup \cdots \cup S_l' \rangle'|,$$  \hspace{1cm} (2.2)

where $(\cdot)$ denotes the subgroup generated by a subset. The answer to Question 1.3 is affirmative if and only if the sum in (2.2) is nonzero. However, to make this sum computable (for all $S$ and $k$), one needs the following data: (i) an enumeration of all subgroups of $G$ and a formula for $|S'|$ for each $S < G$; (ii) for each $S < G$, an enumeration of all immediate supergroups of $S$; (iii) a description of the subgroup generated by any set of immediate supergroups of a subgroup $S$. In the next two sections, we gather these data for $AGL(1, \mathbb{F}_q)$ acting on $\mathbb{F}_q$.

3 The affine linear group $AGL(1, \mathbb{F}_q)$

3.1 The group $AGL(1, \mathbb{F}_q)$

The affine linear group of degree one over $\mathbb{F}_q$ is defined as

$$AGL(1, \mathbb{F}_q) = \left\{ \begin{bmatrix} a & b \\ 0 & 1 \end{bmatrix} : a \in \mathbb{F}_q^*, b \in \mathbb{F}_q \right\} < GL(2, \mathbb{F}_q).$$  \hspace{1cm} (3.1)

The action of $AGL(1, \mathbb{F}_q)$ on $\mathbb{F}_q$ is as follows: For $\begin{bmatrix} a & b \\ 0 & 1 \end{bmatrix} \in AGL(1, \mathbb{F}_q)$ and $x \in \mathbb{F}_q$,

$$\begin{bmatrix} a & b \\ 0 & 1 \end{bmatrix} x = ax + b.$$  \hspace{1cm} (3.2)

This is clearly a sharply 2-transitive action. Let

$$A = \left\{ \begin{bmatrix} a & 0 \\ 0 & 1 \end{bmatrix} : a \in \mathbb{F}_q^* \right\} \cong \mathbb{F}_q^*$$  \hspace{1cm} (3.3)
and
\[ B = \left\{ \begin{bmatrix} 1 & b \\ 0 & 1 \end{bmatrix} : b \in \mathbb{F}_q \right\} \cong \mathbb{F}_q. \] (3.4)

Then we have
\[ \text{AGL}(1, \mathbb{F}_q) = A \rtimes B. \] (3.5)

We list a few formulas that are frequently used as we proceed:
\[ \begin{bmatrix} a & b \\ 0 & 1 \end{bmatrix}^{-1} = \begin{bmatrix} a^{-1} & -a^{-1}b \\ 0 & 1 \end{bmatrix}, \] (3.6)
\[ \begin{bmatrix} a & b \\ 0 & 1 \end{bmatrix}^l = \begin{bmatrix} a^l & a^l - 1 \cdot b \\ 0 & 1 \end{bmatrix}, \quad l \in \mathbb{Z}, \quad \left( \frac{a^l - 1}{a - 1} \right) \text{ interpreted as } l \text{ for } a = 1, \] (3.7)
\[ \begin{bmatrix} a_1 & (a_1 - 1) \cdot b \\ 0 & 1 \end{bmatrix} \begin{bmatrix} a_2 & (a_2 - 1) \cdot b \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} a_1 a_2 & (a_1 a_2 - 1) \cdot b \\ 0 & 1 \end{bmatrix}. \] (3.8)

### 3.2 Subgroups of AGL(1, \mathbb{F}_q)

For \( a \in \mathbb{F}_q^* \), \( b \in \mathbb{F}_q \), and \( H < \mathbb{F}_q \), define
\[ \overline{H} = \left\{ \begin{bmatrix} 1 & h \\ 0 & 1 \end{bmatrix} : h \in H \right\} \] (3.9)
and
\[ S(a, b, H) = \left\{ \begin{bmatrix} a & b \\ 0 & 1 \end{bmatrix} \cup \overline{H} \right\} < \text{AGL}(1, \mathbb{F}_q). \] (3.10)

We fix a generator \( \gamma \) of \( \mathbb{F}_q^* \) and let \( \Gamma = \{ \gamma^i : i \mid q - 1 \} \). Each subgroup of \( \mathbb{F}_q^* \) has a unique generator in \( \Gamma \). Let \( p = \text{char} \mathbb{F}_q \). Let \( S \) be the set of triples \( (a, b, H) \), where \( a \in \Gamma \), \( H \) is an \( \mathbb{F}_p(a) \)-subspace of \( \mathbb{F}_q \), and
\[ b \begin{cases} = 0 & \text{if } a = 1, \\ \in \mathbb{F}_q & \text{if } a \neq 1. \end{cases} \]

For \( (a, b, H) \in S \) and \( h \in H \), we have
\[ \begin{bmatrix} a & b \\ 0 & 1 \end{bmatrix} \begin{bmatrix} 1 & h \\ 0 & 1 \end{bmatrix} \begin{bmatrix} a & b \\ 0 & 1 \end{bmatrix}^{-1} = \begin{bmatrix} 1 & ah \\ 0 & 1 \end{bmatrix} \in \overline{H} \] (3.11)
since \( ah \in H \). Moreover, by (3.7),
\[ \left\{ \begin{bmatrix} a & b \\ 0 & 1 \end{bmatrix} \right\} \cap \overline{H} = \left\{ \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \right\}. \]

Hence
\[ S(a, b, H) = \left\{ \begin{bmatrix} a & b \\ 0 & 1 \end{bmatrix} \right\} \lhd \overline{H}. \] (3.12)

Equation (3.7) also implies that
\[ o \left( \begin{bmatrix} a & b \\ 0 & 1 \end{bmatrix} \right) = o(a), \] (3.13)
where \( o(\ ) \) denotes the order of an element in a group. Thus
\[
|S(a, b, H)| = o(a)|H|.
\]
(3.14)

**Theorem 3.1** Every subgroup of AGL(1, \( \mathbb{F}_q \)) is of the form \( S(a, b, H) \) for some \( (a, b, H) \in S \).

**Proof** Let \( S < \text{AGL}(1, \mathbb{F}_q) \). We have an embedding
\[
S/S \cap B \rightarrow \text{AGL}(1, \mathbb{F}_q)/B \cong \mathbb{F}_q^*,
\]
where \( B \) is given in (3.4). Write \( S \cap B = \overline{H} \) for some \( H < \mathbb{F}_q \). By (3.15), \( S/\overline{H} \) is cyclic with \( |S/\overline{H}| \mid q - 1 \). Write
\[
S/\overline{H} = \left[ \begin{bmatrix} a & b \\ 0 & 1 \end{bmatrix} \right] \overline{H}, \quad \text{where } \begin{bmatrix} a & b \\ 0 & 1 \end{bmatrix} \in S.
\]
(3.16)

Since \( \begin{bmatrix} a & b \\ 0 & 1 \end{bmatrix} \in \overline{H} \) if and only if \( a^n = 1 \), we have \( |S/\overline{H}| = o(a) \). There exists \( a' \in \Gamma \) such that \( \langle a \rangle = \langle a' \rangle \), that is, \( a' = a^l \) for some \( l \in \mathbb{Z} \) with \( \gcd(l, o(a)) = 1 \). Then
\[
S/\overline{H} = \left[ \begin{bmatrix} a & b \\ 0 & 1 \end{bmatrix} \right]^{l} = \left[ \begin{bmatrix} a' & 0 \\ 0 & 1 \end{bmatrix} \right] \overline{H}.
\]

Hence we may assume that \( a \in \Gamma \) in (3.16). Since
\[
\begin{bmatrix} a & b \\ 0 & 1 \end{bmatrix} \overline{H} = \begin{bmatrix} a & b \\ 0 & 1 \end{bmatrix} \overline{H}^{-1} = \overline{H},
\]
it follows from (3.11) that \( aH = H \). Hence \( H \) is an \( \mathbb{F}_p(a) \)-subspace of \( \mathbb{F}_q \). If \( a = 1 \), by (3.16), \( S/\overline{H} \) is a \( p \)-group. Then \( |S/\overline{H}| = 1 \), and hence \( S = \overline{H} = S(1, 0, H) \), where \( (1, 0, H) \in S \).

If \( a \neq 1 \), then \( (a, b, H) \in S \) and
\[
S = \left\{ \begin{bmatrix} a & b \\ 0 & 1 \end{bmatrix} \cup \overline{H} \right\} = S(a, b, H).
\]

\[ \square \]

**Proposition 3.2** (i) For \( (a_1, b_1, H_1), (a_2, b_2, H_2) \in S \), \( S(a_1, b_1, H_1) = S(a_2, b_2, H_2) \) if and only if \( H_1 = H_2, a_1 = a_2, \) and \( b_1 \equiv b_2 \pmod{H_1} \).

(ii) For each \( (a, b, H) \in S \), there exists \( c \in \mathbb{F}_q \) such that
\[
\begin{bmatrix} 1 & c \\ 0 & 1 \end{bmatrix} S(a, b, H) \begin{bmatrix} 1 & c \\ 0 & 1 \end{bmatrix}^{-1} = S(a, 0, H).
\]
(3.17)

**Proof** (i) \( \iff \) This simply follows from the fact that
\[
\begin{bmatrix} a_1 & b_1 \\ 0 & 1 \end{bmatrix}^{-1} \begin{bmatrix} a_1 & b_2 \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} 1 & (b_2 - b_1)/a_1 \\ 0 & 1 \end{bmatrix} \in \overline{H_1}.
\]

(\( \Rightarrow \)) For \( i = 1, 2, \overline{H}_i \) is the unique Sylow \( p \)-subgroup of \( S(a_i, b_i, H_i) \). Since \( S(a_1, b_1, H_1) = S(a_2, b_2, H_2) \), we have \( \overline{H_1} = \overline{H_2} \) and hence \( H_1 = H_2 \). It follows from \( |S(a_1, b_1, H_1)| = |S(a_2, b_2, H_1)| \) that \( o(a_1) = o(a_2) \). Since \( a_1, a_2 \in \Gamma \), we must have \( a_1 = a_2 \).

Since
\[
\begin{bmatrix} a_1 & b_1 \\ 0 & 1 \end{bmatrix} \overline{H_1} = S(a_1, b_1, H_1)/\overline{H_1} = S(a_1, b_2, H_1)/\overline{H_1} = \begin{bmatrix} a_1 & b_2 \\ 0 & 1 \end{bmatrix} \overline{H_1},
\]
\[ \square \] Springer
there exists $0 < l \leq o(a_1)$ such that
\[
\begin{bmatrix} a_1 & b_1 \\ 0 & 1 \end{bmatrix}^l H_1 = \begin{bmatrix} a_1 & b_2 \\ 0 & 1 \end{bmatrix} H_1.
\]

It follows that $a_1^l = a_1$ and hence $l = 1$. Now from
\[
\begin{bmatrix} a_1 & b_1 \\ 0 & 1 \end{bmatrix} H_1 = \begin{bmatrix} a_1 & b_2 \\ 0 & 1 \end{bmatrix} H_1
\]
we have $b_1 \equiv b_2 \pmod{H_1}$.

(ii) Let
\[
c = \begin{cases} 0 & \text{if } a = 1, \\ b & \text{if } a \neq 1. \\ a - 1 \end{cases}
\]

Then
\[
\begin{bmatrix} 1 & c \\ 0 & 1 \end{bmatrix} \begin{bmatrix} a & b \\ 0 & 1 \end{bmatrix} \begin{bmatrix} 1 & c \\ 0 & 1 \end{bmatrix}^{-1} = \begin{bmatrix} a - (1 - a)c + b \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} a & 0 \\ 0 & 1 \end{bmatrix}.
\]

Of course,
\[
\begin{bmatrix} 1 & c \\ 0 & 1 \end{bmatrix} H \begin{bmatrix} 1 & c \\ 0 & 1 \end{bmatrix}^{-1} = H.
\]

Hence (3.17) holds. \hfill \Box

**Proposition 3.3** Let $(a, 0, H) \in S$.

(i) If $a = 1$, the subgroups of $AGL(1, \mathbb{F}_q)$ that contain $S(1, 0, H) = H$ are precisely $S(a_1, b_1, H_1)$, where $(a_1, b_1, H_1) \in S$, $H \subset H_1$.

(ii) If $a \neq 1$, the subgroups of $AGL(1, \mathbb{F}_q)$ that contain $S(a, 0, H)$ are precisely $S(a_1, 0, H_1)$, where $(a_1, 0, H_1) \in S$, $a \in \langle a_1 \rangle$, $H \subset H_1$.

**Proof** (i) By Theorem 3.1, each subgroup of $AGL(1, \mathbb{F}_q)$ is of the form $S(a_1, b_1, H_1)$ defined in (3.10), where $(a_1, b_1, H_1) \in S$. Note that $S(a_1, b_1, H_1) \supset H$ if and only if the Sylow $p$-subgroup of $S(a_1, b_1, H_1)$, $H_1$, contains $H$.

(ii) First assume that $(a_1, 0, H_1) \in S$ is such that $a \in \langle a_1 \rangle$ and $H \subset H_1$. Then $H \subset H_1$ and $\begin{bmatrix} a & 0 \\ 0 & 1 \end{bmatrix} \in \langle \begin{bmatrix} a_1 & 0 \\ 0 & 1 \end{bmatrix} \rangle$. Hence $S(a, 0, H) \subset S(a_1, 0, H_1)$.

Now assume that $S(a, 0, H) \subset S(a_1, b_1, H_1)$, where $(a_1, b_1, H_1) \in S$. Since $H$ is a $p$-subgroup of $S(a_1, b_1, H_1)$, we have $H \subset H_1$, and hence $H \subset H_1$. Since $\begin{bmatrix} a & 0 \\ 0 & 1 \end{bmatrix} \in S(a_1, b_1, H_1)$, there exists integer $l > 0$ such that
\[
\begin{bmatrix} a & 0 \\ 0 & 1 \end{bmatrix}^l \in \begin{bmatrix} a_1 & b_1 \\ 0 & 1 \end{bmatrix} H_1.
\]

Then $a_1^l = a$ and (3.18) becomes
\[
\begin{bmatrix} a & 0 \\ 0 & 1 \end{bmatrix} \in \begin{bmatrix} a & b_1(a - 1)/(a_1 - 1) \\ 0 & 1 \end{bmatrix} H_1.
\]

Thus $b_1(a - 1)/(a_1 - 1) \in H_1$, whence $b_1 \in H_1$ since $H_1$ is an $\mathbb{F}_p(a_1)$-space. We then have $S(a_1, b_1, H_1) = S(a_1, 0, H_1)$. \hfill \Box
3.3 Orbits of $S(a, b, H)$

Let $(a, b, H) \in S$. If $a = 1$, the orbits of $S(1, 0, H) = \overline{H}$ in $\mathbb{F}_q$ are clearly the cosets of $H$ in $\mathbb{F}_q$.

Now assume that $a \neq 1$. Let $\sigma = \left[ \begin{array}{cc} a & b \\ 1 & 1 \end{array} \right]$. If $x, y \in \mathbb{F}_q$ are such that $x \equiv y \pmod{H}$, then $\sigma(x) - \sigma(y) = a(x - y) \equiv 0 \pmod{H}$. Moreover, for all $\beta \in \overline{H}$ and $x \in \mathbb{F}_q$, $\beta x \equiv x \pmod{H}$. Hence the action of $S(a, b, H)$ on $\mathbb{F}_q$ induces an action of $S(\sigma(a, b, H)/\overline{H}) \cong \langle \sigma \rangle$ on $\mathbb{F}_q/H$. For all $0 \leq l < o(a)$ and $x \in \mathbb{F}_q$,

$$\sigma^l x = a^l x + b(a^l - 1)/(a - 1).$$

Note that $\sigma^l x \equiv x \pmod{H}$ if and only if $x \equiv -b/(a - 1) \pmod{H}$. Therefore, the $\langle \sigma \rangle$-orbits in $\mathbb{F}_q/H$ containing $x + H$ are

$$\begin{cases} \{x + H\} & \text{if } x + H = -b/(a - 1) + H, \\ \{a^l x + b(a^l - 1)/(a - 1) + H : 0 \leq l < o(a)\} & \text{otherwise}. \end{cases}$$

Consequently, the $S(a, b, H)$-orbit in $\mathbb{F}_q$ containing $x$ is

$$\begin{cases} x + H & \text{if } x \equiv -b/(a - 1) \pmod{H}, \\ \bigcup_{0 \leq l < o(a)} \{a^l x + b(a^l - 1)/(a - 1) + H\} & \text{otherwise}. \end{cases}$$

Note that $S(a, b, H)$ has one orbit of size $|H|$ and $(q - |H|)/o(a)|H|$ orbits of size $o(a)|H|$ in $\mathbb{F}_q$.

Subsets of $\mathbb{F}_q$ that are set-wise fixed by $S(a, b, H)$ are precisely unions of $S(a, b, H)$-orbits in $\mathbb{F}_q$. Hence the preceding discussion yields the following proposition.

**Proposition 3.4** Let $0 \leq k \leq q$ be fixed and $(\cdot)^\prime$ be defined in (2.1). Let $(a, b, H) \in S$.

(i) If $a = 1$,

$$|S(1, 0, H)^\prime| = \begin{cases} \frac{(q/|H|)}{k/|H|} & \text{if } k \equiv 0 \pmod{|H|}, \\ 0 & \text{otherwise}. \end{cases}$$

(ii) If $a \neq 1$,

$$|S(a, b, H)^\prime| = \begin{cases} \frac{(q - |H|)/o(a)|H|}{k/|H|} & \text{if } k \equiv 0 \pmod{o(a)|H|}, \\ \frac{(q - |H|)/o(a)|H|}{(k - |H|)/o(a)|H|} & \text{if } k \equiv |H| \pmod{o(a)|H|}, \\ 0 & \text{otherwise}. \end{cases}$$

For integers $u, v > 0$, define

$$s_{q,k}(u, v) = \left(\frac{(q - v)/uv}{k/uv}\right) + \left(\frac{(q - v)/uv}{(k - v)/uv}\right),$$

where a binomial coefficient $\binom{y}{\cdot}$ is defined to be 0 if $y \notin \mathbb{N}$. Then (3.19) and (3.20) can be combined as

$$|S(a, b, H)^\prime| = s_{q,k}(o(a), |H|) \quad \text{for all } (a, b, H) \in S.$$  (3.22)

**Remark 3.5** We have $s_{q,k}(u, v) = 0$ unless $k \equiv 0$ or $v \pmod{uv}$.  

Springer
4 A solution to question 1.3 for $AGL(1, \mathbb{F}_q)$

First, we need to extend our notation. Let $q = p^n$. For any $d \in \mathbb{Z}$ with $p \nmid d$, let $\omega_d(p)$ denote the order of $p$ in $\mathbb{Z}_d^\times$, and let $p(d) = p^{\omega_d(p)}$, which is the smallest power of $p$ that is $\equiv 1$ (mod $d$). For a vector space $V$ over a field $K$, let $\mathbb{F}_K(V)$ be the set of all one-dimensional subspaces of $V$. For each $H < \mathbb{F}_q$, let $H^1 = \{x \in \mathbb{F}_q : xH \subset H\}$, which is the largest subspace of $\mathbb{F}_q$ such that $H$ is a $K$-module. For each subset $X \subset \mathbb{F}_q$, let $\langle X \rangle_K$ denote the $K$-span of $X$. For each positive integer $n$, let $\mathcal{P}(n)$ denote the set of all prime divisors of $n$. If $P \subset \mathbb{Z}$ is finite, define $\Pi P = \prod_{e \in P} e$. Recall that $\gamma$ is a fixed generator of $\mathbb{F}_q^\times$.

Let $\mu(\cdot, \cdot)$ denote the Möbius function of the partially ordered set of all finite dimensional subspaces of a vector space over $\mathbb{F}_q$. It is well known [2] that if $W \subset V$ are finite dimensional vector spaces over $\mathbb{F}_q$, then

$$\mu_q(W, V) = (-1)^{\dim_{\mathbb{F}_q}(V/W)} q^\left(\frac{\dim_{\mathbb{F}_q}(V/W)}{2}\right).$$  \hspace{1cm} (4.1)

Recall that the number of $m$-dimensional $\mathbb{F}_q$-subspaces of an $n$-dimensional $\mathbb{F}_q$-vector space is given by the $q$-binomial coefficient

$$\binom{n}{m}_q = \prod_{i=0}^{m-1} \frac{1 - q^{n-i}}{1 - q^{i+1}}. \hspace{1cm} (4.2)$$

Given $S < AGL(1, \mathbb{F}_q)$ and $0 \leq k \leq q$, let

$$\mathcal{N}(S, k) = \left| \left\{ B \in \binom{\mathbb{F}_q}{k} : S = AGL(1, \mathbb{F}_q)_B \right\} \right|. \hspace{1cm} (4.3)$$

Obviously,

$$\mathcal{N}(S, k) \leq |S'|, \hspace{1cm} (4.4)$$

but the equality does not hold in general. The objective of this section is to determine $\mathcal{N}(S, k)$. By Theorem 3.1 and Proposition 3.2, it suffices to consider $S = S(\gamma(q-1)/d, 0, H)$, where $d \mid q - 1$ and $(\gamma(q-1)/d, 0, H) \in S$. Since $AGL(1, \mathbb{F}_q)_B = AGL(1, \mathbb{F}_q)_{\mathbb{F}_q \setminus B}$, we also have

$$\mathcal{N}(S, q - k). \hspace{1cm} (4.5)$$

Hence it suffices to consider $0 \leq k \leq q/2$.

4.1 The case $S = S(1, 0, H)$

Consider $S = S(1, 0, H)$, where $(1, 0, H) \in S$. Let $\phi : \mathbb{F}_q \rightarrow \mathbb{F}_q/H$ be the canonical homomorphism and let $B$ be a system of coset representatives of $H$ in $\mathbb{F}_q$. By Proposition 3.3, the immediate supergroups of $S(1, 0, H)$ in $AGL(1, \mathbb{F}_q)$ are precisely

$$S(\gamma(q-1)/e, b, H), \hspace{1cm} e \in \mathcal{P}(|H^1| - 1), \hspace{0.2cm} b \in B, \hspace{1cm} (4.6)$$

and

$$S(1, 0, \phi^{-1}(x)), \hspace{1cm} x \in \mathbb{F}_p(\mathbb{F}_q/H). \hspace{1cm} (4.7)$$
Let $C \subset \mathcal{P}(H^+) - 1 \times B$ and $X \subset \mathbb{F}_p(\mathbb{F}_q/H)$ be arbitrary. Define
\[
B(C) = \left\{ \frac{b}{\gamma(q-1)/e - 1} : (e, b) \in C \right\}
\]
and
\[
\Delta(C) = \{ u - v : u, v \in B(C) \}.
\]
Write
\[
C = \bigcup_{e \in P}(e \times B_e),
\]
where $P \subset \mathcal{P}(H^+) - 1$ and $\emptyset \neq B_e \subset B$ for all $e \in P$.

**Lemma 4.1** In the above notation we have
\[
\left( S(1, 0, H) \cup \left( \bigcup_{(e, b) \in C} S(\gamma(q-1)/e, b, H) \right) \right) \cup \left( \bigcup_{x \in X} S(1, 0, \phi^{-1}(x)) \right) = S(\gamma(q-1)/\Pi P, (\gamma(q-1)/\Pi P - 1)u, \left( \Delta(C) \cup H \cup \left( \bigcup_{x \in X} \phi^{-1}(x) \right) \right)_{\mathbb{F}(\Pi P)},
\]
where $u \in B(C)$ is arbitrary. (Note that when $C = \emptyset, \gamma(q-1)/\Pi P - 1 = 0$ and $u$ is irrelevant.)

**Proof** Let $L$ and $R$ denote the left and right sides of (4.11), respectively. Note that $\mathbb{F}_p(\gamma(q-1)/\Pi P) = \mathbb{F}_p(\Pi P)$; hence the triple of parameters in $R$ belongs to $S$.

1° We first show that $L \subset R$. Let
\[
H_1 = \left( \Delta(C) \cup H \cup \left( \bigcup_{x \in X} \phi^{-1}(x) \right) \right)^{\overline{F}(\Pi P)}.
\]
For each $x \in X$, clearly, $S(1, 0, \phi^{-1}(x)) \subset H_1 \subset R$. Moreover, for each $(e, b) \in C$, we have
\[
R \ni \begin{bmatrix} \gamma(q-1)/\Pi P & (\gamma(q-1)/\Pi P - 1)u \\ 0 & 1 \end{bmatrix}^{(\Pi P)/e}
\]
\[
= \begin{bmatrix} \gamma(q-1)/e & \gamma(q-1)/e - 1 \\ 0 & 1 \end{bmatrix}^{\gamma(q-1)/\Pi P - 1}(\gamma(q-1)/\Pi P - 1)u
\]
\[
= \begin{bmatrix} \gamma(q-1)/e & (\gamma(q-1)/e - 1)u \\ 0 & 1 \end{bmatrix}
\]
\[
\in \begin{bmatrix} \gamma(q-1)/e & b \\ 0 & 1 \end{bmatrix}^{\overline{H}_1} \quad (\text{since } u - \frac{b}{\gamma(q-1)/e - 1} \in H_1)
\]
\[
= \begin{bmatrix} \gamma(q-1)/e & b \\ 0 & 1 \end{bmatrix}^{\overline{H}_1}.
\]
Thus $L \subset R$.

2° Now we show that $R \subset L$. Let $\overline{H}_1$ be the Sylow $p$-subgroup of $L$, where $H_1 < \mathbb{F}_q$. Enumerate the elements of $C$ as $(e_1, b_1), \ldots, (e_l, b_l)$. Since $\gcd((q - 1)/e_i : 1 \leq i \leq l) = (q - 1)/\Pi P$, we have
\[
\sum_{i=1}^{l} \frac{q - 1}{e_i} = \frac{q - 1}{\Pi P}.
\]
Thus (4.12). In fact, we have

\[ L \ni \begin{bmatrix} \gamma^{(q-1)/e_1} b_1 \\ 0 \\ 1 \end{bmatrix} \cdots \begin{bmatrix} \gamma^{(q-1)/e_l} b_l \\ 0 \\ 1 \end{bmatrix} = \begin{bmatrix} \gamma^\sum_{i=1}^l a_i (q-1)/e_i \\ 0 \\ 1 \end{bmatrix} = \begin{bmatrix} \gamma^{(q-1)/\Pi P} \\ 0 \\ 1 \end{bmatrix}. \tag{4.12} \]

It follows that \( H_1 \) is an \( \mathbb{F}_p(\Pi P) \)-subspace of \( \mathbb{F}_q \).

Clearly, \( \bigcup_{x \in X} \phi^{-1}(x) \subset H_1 \). Let \( a_i = \gamma^{(q-1)/e_i}, 1 \leq i \leq l \). Then for \( 1 \leq i, j \leq l \),

\[ L \ni \begin{bmatrix} a_i b_i \\ a_j b_j \\ a_i b_i \end{bmatrix} = \begin{bmatrix} 1 \\ 0 \\ 1 \end{bmatrix} - (a_i - 1)b_j - (a_j - 1)b_i. \]

Thus \( (a_i - 1)b_j - (a_j - 1)b_i \in H_1 \), i.e., \( b_i/(a_i - 1) - b_j/(a_j - 1) \in H_1 \). Hence \( \Delta(C) \subset H_1 \). Therefore

\[ \left( \Delta(C) \cup H \cup \left( \bigcup_{x \in X} \phi^{-1}(x) \right) \right)^{\mathbb{F}_p(\Pi P)} \subset H_1. \tag{4.13} \]

Next, we take a closer look of (4.12). In fact, we have

\[ L \ni \begin{bmatrix} a_1 b_1 \\ 0 \\ 1 \end{bmatrix}^{\alpha_1} \cdots \begin{bmatrix} a_l b_l \\ 0 \\ 1 \end{bmatrix}^{\alpha_l} = \begin{bmatrix} a_1^{\alpha_1} (a_1^{\alpha_1} - 1)b_1/(a_1 - 1) \\ 0 \\ 1 \end{bmatrix} \cdots \begin{bmatrix} a_l^{\alpha_l} (a_l^{\alpha_l} - 1)b_l/(a_l - 1) \\ 0 \\ 1 \end{bmatrix} = \begin{bmatrix} a_1^{\alpha_1} \cdots a_l^{\alpha_l} (a_1^{\alpha_1} \cdots a_l^{\alpha_l} - 1)u \\ 0 \\ 1 \end{bmatrix} \overline{H}_1. \]

Hence

\[ \begin{bmatrix} \gamma^{(q-1)/\Pi P} \\ 0 \\ 1 \end{bmatrix} \begin{bmatrix} \gamma^{(q-1)/\Pi P} \\ 0 \\ 1 \end{bmatrix} - (\gamma^{(q-1)/\Pi P} - 1)u \in L. \tag{4.14} \]

By (4.13) and (4.14), \( R \subset L \).

\[ \square \]

**Theorem 4.2** Let \( (1, 0, H) \in S \) and let \( |H| = p^\beta \). Then for \( 0 \leq k \leq q \),

\[ \mathcal{N}(S(1, 0, H), k) = (1 - p^{\alpha - \beta}) \sum_{0 \leq l \leq \alpha - \beta} (-1)^l p^{\binom{l}{2}} \begin{bmatrix} \alpha - \beta \\ l \end{bmatrix} s_{q,k}(1, p^{\beta+l}) + p^{\alpha - \beta} \sum_{P \subset P(H^l|1)} \sum_{0 \leq l \leq (\alpha - \beta)/o_{\Pi P}(p)} (-1)^{|P|+l} p(\Pi P)^{\binom{l}{2}} \begin{bmatrix} (\alpha - \beta)/o_{\Pi P}(p) \\ l \end{bmatrix} p(\Pi P) \cdot s_{q,k}(\Pi P, p^{\beta+l}o_{\Pi P}(p)) \tag{4.15} \]
By (4.3), (2.2), (4.11), and (3.22), we have

\[ \mathcal{N}(S(1, 0, H), k) = \sum_{C \subset \mathcal{P}(|H^\perp| - 1) \times \mathcal{B}} (-1)^{|C| + |X|} s_{q,k}(\Pi P, \left| \Delta(C) \cup H \cup \left( \bigcup_{x \in X} \phi^{-1}(x) \right) \right|^{F_{\rho(P)}} \right). \]  

(Note that in (4.16), \( P \subset \mathcal{P}(|H^\perp| - 1) \) is given by (4.10) and is dependent on \( C \).) In what follows, we simplify (4.16) to a more computable form. Rewrite (4.16) as

\[ \mathcal{N}(S(1, 0, H), k) = \sum_{C \subset \mathcal{P}(|H^\perp| - 1) \times \mathcal{B}} (-1)^{|C|} s_{q,k}(\Pi P, |U|) \sum_{X \subset \mathcal{P}_p(F_q/H)} (-1)^{|X|} \mathcal{N}(\Delta(C) \cup H \cup (\bigcup_{x \in X} \phi^{-1}(x))^{F_{\rho(P)}}, U). \]  

Let \( C \) and \( U \) in the outer sum of (4.17) be fixed. For each \( F_{\rho(P)} \)-module \( V \) with \( \Delta(C) \cup H \subset V \subset U \), define

\[ f(V) = \sum_{X \subset \mathcal{P}_p(F_q/H)} (-1)^{|X|} \mathcal{N}((\Delta(C) \cup H \cup (\bigcup_{x \in X} \phi^{-1}(x)))^{F_{\rho(P)}}, U). \]  

and

\[ f_\leq(V) = \sum_{W: F_{\rho(P)}-module \quad \Delta(C) \cup H \subset W \subset V} f(W). \]  

Then

\[ f_\leq(V) = \sum_{X \subset \mathcal{P}_p(F_q/H)} (-1)^{|X|} \begin{cases} 1 & \text{if } V = H, \\ 0 & \text{if } V \supsetneq H. \end{cases} \]  

By the Möbius inversion,

\[ f(V) = \sum_{W: F_{\rho(P)}-module \quad \Delta(C) \cup H \subset W \subset V} \mu_p(\Pi P, W, V) f_\leq(W) = \begin{cases} \mu_p(\Pi P, H, V) & \text{if } \Delta(C) \subset H, \\ 0 & \text{if } \Delta(C) \not\subset H. \end{cases} \]  

Therefore (4.17) becomes

\[ \mathcal{N}(S(1, 0, H), k) = \sum_{C \subset \mathcal{P}(|H^\perp| - 1) \times \mathcal{B}, \Delta(C) \subset H} (-1)^{|C|} s_{q,k}(\Pi P, |U|) \mu_p(\Pi P, H, U). \]  

Each \( \emptyset \neq C \subset \mathcal{P}(|H^\perp| - 1) \times \mathcal{B} \) with \( \Delta(C) \subset H \) is obtained in the following way: First choose \( \emptyset \neq P \subset \mathcal{P}(|H^\perp| - 1) \) and a coset \( u + H \), where \( u \in \mathcal{B} \). Then choose \( C = \{(e, b_e) : e \in P\} \), where \( b_e \in \mathcal{B} \) is the unique element such that \( b_e/(y^{(q-1)/e} - 1) \in u + H \). Therefore, (4.22) can be written as

\[ \mathcal{N}(S(1, 0, H), k) = \sum_{C \subset \mathcal{P}(|H^\perp| - 1) \times \mathcal{B}, \Delta(C) \subset H} (-1)^{|C|} s_{q,k}(\Pi P, |U|) \mu_p(\Pi P, H, U). \]  

\[ \left(4.22\right) \]
\[ \mathcal{N}(S(1, 0, H), k) \]
\[ = \sum_{U: \mathbb{F}_p\text{-module, } H \subset U \subset \mathbb{F}_q} s_{q, k}(1, |U|) \mu_p(H, U) \]
\[ + \sum_{\emptyset \neq P \subset \mathcal{P}(|H| - 1)} \frac{q}{|H|} (-1)^{|P|} s_{q, k}(\Pi P, |U|) \mu_p(\Pi P)(H, U). \]  
\[ (4.23) \]

Let \( l = \dim_{\mathbb{F}_p(\Pi P)} (U / H) \). Then
\[ \mu_p(\Pi P)(H, U) = (-1)^l p(\Pi P)^{\ell \frac{l}{2}}, \]
and (4.23) becomes
\[ \mathcal{N}(S(1, 0, H), k) \]
\[ = \sum_{0 \leq l \leq \alpha - \beta} (-1)^l p^{\ell \frac{l}{2}} \left[ \alpha - \beta \right]_p s_{q, k}(1, p^{\beta+l}) \]
\[ + p^{\alpha - \beta} \sum_{\emptyset \neq P \subset \mathcal{P}(|H| - 1)} \sum_{0 \leq l \leq \alpha - \beta / o_{\Pi P}(p)} (-1)^{|P|+l} p(\Pi P)^{\ell \frac{l}{2}} \left[ (\alpha - \beta) / o_{\Pi P}(p) \right]_p \]
\[ \cdot s_{q, k}(\Pi P, p^{\beta+l/ o_{\Pi P}(p)}). \]

\[ \Box \]

### 4.2 The case \( S = S(\gamma^{(q-1)/d}, 0, H) \), where \( d > 1 \) and \( d \mid q - 1 \)

Let \( (\gamma^{(q-1)/d}, 0, H) \in S \), where \( d > 1 \) and \( d \mid q - 1 \). The computation of \( \mathcal{N}(S(\gamma^{(q-1)/d}, 0, H), k) \) is similar to Sect. 4.1. By Proposition 3.3 (ii), the immediate supergroups of \( S(\gamma^{(q-1)/d}, 0, H) \) in \( AGL(1, \mathbb{F}_q) \) are precisely
\[ S(\gamma^{(q-1)/de}, 0, H), \quad e \in \mathcal{P} \left( \frac{|H| - 1}{d} \right), \]  
\[ (4.24) \]
and
\[ S(\gamma^{(q-1)/d}, 0, \phi^{-1}(x)), \quad x \in \mathbb{F}_{p(d)}(\mathbb{F}_q / H). \]  
\[ (4.25) \]

**Lemma 4.3** Let \( d > 1 \) be a divisor of \( q - 1 \), \( P \subset \mathcal{P}((|H| - 1)/d) \) and \( X \subset \mathbb{F}_{p(d)}(\mathbb{F}_q / H) \).
Then
\[ \left( S(\gamma^{(q-1)/d}, 0, H) \cup \left( \bigcup_{e \in P} S(\gamma^{(q-1)/de}, 0, H) \right) \cup \left( \bigcup_{x \in X} S(\gamma^{(q-1)/d}, 0, \phi^{-1}(x)) \right) \right) \]
\[ = S(\gamma^{(q-1)/d} \Pi P, 0, \left( H \cup \left( \bigcup_{x \in X} \phi^{-1}(x) \right) \right)^{\mathbb{F}_{p(d)\Pi P}}). \]  
\[ (4.26) \]

**Proof** The proof of Lemma 4.3 is similar to but simpler than that of Lemma 4.1. We leave the details for the reader. \( \Box \)

**Theorem 4.4** Let \( (\gamma^{(q-1)/d}, 0, H) \in S \), where \( d > 1 \) and \( d \mid q - 1 \), and let \( |H| = p^\beta \). Then for \( 0 \leq k \leq q \).

\[ \Box \]
\[ N(S(γ^{q-1}/d, 0, H), k) \]
\[ = \sum_{P \subseteq \mathcal{P}((|H'|-1)/d)} \sum_{0 \leq l \leq (α - β)/\alpha_{d} \cap P(p)} (-1)^{|P|+l} p(d \Pi P)^{(l)} \begin{bmatrix} (α - β)/\alpha_{d} \cap P(p) \\ l \end{bmatrix}_{p \cap (d \Pi P)} \cdot s_{q,k}(d \Pi P, \ b^{\beta} + 1+ \alpha_{d} \cap P(p)). \tag{4.27} \]

**Proof** By (4.3), (2.2), (4.26), and (3.22),
\[ N(S(γ^{q-1}/d, 0, H), k) \]
\[ = \sum_{P \subseteq \mathcal{P}((|H'|-1)/d)} \sum_{X \subseteq \mathbb{F}_{p \cap (d \Pi P)}-(\mathbb{F}_{q}/H)} (-1)^{|X|} s_{q,k}(d \Pi P, |X|) \left( H \bigcup \left( \bigcup_{x \in X} \phi^{-1}(x) \right)^{(H \cap (\bigcup_{x \in X} \phi^{-1}(x)))_{p \cap (d \Pi P)}=U} \right) \]
\[ = \sum_{P \subseteq \mathcal{P}((|H'|-1)/d)} \sum_{X \subseteq \mathbb{F}_{p \cap (d \Pi P)}-(\mathbb{F}_{q}/H)} (-1)^{|X|}. \tag{4.28} \]

By the same argument that led to (4.21), we find that the inner sum in (4.28) equals \( \mu_{p \cap (d \Pi P)}(H, U) \). Hence
\[ N(S(γ^{q-1}/d, 0, H), k) \]
\[ = \sum_{P \subseteq \mathcal{P}((|H'|-1)/d)} \sum_{U : \mathbb{F}_{p \cap (d \Pi P)}-\text{module}} (-1)^{|P|} s_{q,k}(d \Pi P, |U|) \mu_{p \cap (d \Pi P)}(H, U). \tag{4.29} \]

Let \( l = \text{dim}_{\mathbb{F}_{p \cap (d \Pi P)}}(U/H) \). Then
\[ N(S(γ^{q-1}/d, 0, H), k) \]
\[ = \sum_{P \subseteq \mathcal{P}((|H'|-1)/d)} \sum_{0 \leq l \leq (α - β)/\alpha_{d} \cap P(p)} (-1)^{|P|+l} p(d \Pi P)^{(l)} \begin{bmatrix} (α - β)/\alpha_{d} \cap P(p) \\ l \end{bmatrix}_{p \cap (d \Pi P)} \cdot s_{q,k}(d \Pi P, \ b^{\beta} + 1+ \alpha_{d} \cap P(p)). \]

\( \square \)

**Corollary 4.5** If \( N(S(γ^{q-1}/d, 0, H), k) > 0 \), where \( d \mid q - 1 \) and \( |H| = p^{\beta} \), then
\[ A_{2} \begin{bmatrix} q(q - 1) \\ p^{\beta}d \end{bmatrix}, \begin{bmatrix} 2k(q - k) \\ p^{\beta}d \end{bmatrix}, \begin{bmatrix} k(q - 1) \\ p^{\beta}d \end{bmatrix} = q. \]

**Proof** This follows from (1.6) and the definition of \( N(S(γ^{q-1}/d, 0, H), k) \). \( \square \)

**Remark 4.6** (i) It follows from (4.4), (3.22) and Remark 3.5 that \( N(S(γ^{q-1}/d, 0, H), k) = 0 \) unless \( k \equiv 0 \) or \( p^{\beta} \) (mod \( d p^{\beta} \)), where \( d \mid p - 1 \) and \( |H| = p^{\beta} \).

(ii) Assume that \( k = 0 \) or \( q \). It is clear that
\[ N(S, 0) = N(S, q) = \begin{cases} 1 & \text{if } S = S(γ, 0, \mathbb{F}_{q}), \\ 0 & \text{otherwise}. \end{cases} \tag{4.30} \]
Lemma 5.1

The possible values of precisely but not on $H$. The formulas (4.15) and (4.27) for $5$ Computation of Affine linear groups

Proof

This follows from Lemma 5.2.

Let $H = \langle \gamma \rangle$. Then $S = S(1, 0, H)$. However, to derive (4.30)–(4.32) from (4.15) and (4.27), it requires some computation; we leave the details to the reader.

5 Computation of $N(S(\gamma^{(q-1)/d}), 0, H), k)$

The formulas (4.15) and (4.27) for $N(S(\gamma^{(q-1)/d}), 0, H), k)$ depend on $q, k, d, |H|$ and $|H^\perp|$ but not on $H$. Thus, with $q, k, d$ given, we only have to know the possible pairs of values $(|H|, |H^\perp|)$.

Recall that $q = p^d$ and $\mathbb{F}_q(\gamma^{(q-1)/d}) = \mathbb{F}_{p(d)}$.

Lemma 5.1

The possible values of $(|H|, |H^\perp|)$, where $H \subset \mathbb{F}_q$ is an $\mathbb{F}_{p(d)}$-subspace, are precisely

$(1, q), (q, q)$, and $(p(d)^i, p(d)^i), i \mid (\alpha/\alpha_d(p)), i < \alpha/\alpha_d(p)$, $0 < j < \alpha/\alpha_d(p)i$.

Proof

This follows from Lemma 5.2.

Lemma 5.2

Let $\mathbb{F}_r \subset \mathbb{F}_q$ and $0 \leq d \leq [\mathbb{F}_q : \mathbb{F}_r]$. Then there exists $H < \mathbb{F}_q$ such that $H^\perp = \mathbb{F}_r$, and $\dim_{\mathbb{F}_r} H = d$ if and only if

(i) $[\mathbb{F}_q : \mathbb{F}_r] = 1$, or
(ii) $[\mathbb{F}_q : \mathbb{F}_r] > 1$ and $0 < d < [\mathbb{F}_q : \mathbb{F}_r]$.

\(\square\)
Proof. The proof is essentially the same as that of [16, Theorem 4.14].

(⇒) Obvious.

(⇐) Let \( n = [\mathbb{F}_q : \mathbb{F}_r] \). If \( n = 1 \), let \( H = 0 \) for \( d = 0 \) and \( H = \mathbb{F}_q \) for \( d = 1 \). Assume that \( n > 1 \) and \( 0 < d < n \). Let \( e_1, \ldots, e_l \) be the distinct prime factors of \( n \). Clearly, \( l \leq n - 1 \). Choose \( a_i \in \mathbb{F}_{r^i} \setminus \mathbb{F}_r \), \( 1 \leq i \leq l \). Clearly, \( a_1, \ldots, a_l, a_{l+1}(=1) \) are linearly independent over \( \mathbb{F}_r \). Extend them to an \( \mathbb{F}_r \)-basis \( a_i \), \( 1 \leq i \leq n \), of \( \mathbb{F}_q \). Let \( L = \{ \sum_{i=1}^n x_i a_i : x_i \in \mathbb{F}_r, \ x_1 + \cdots + x_i = 0 \} \subset \mathbb{F}_q \). Then \( \dim_{\mathbb{F}_r} L = n - 1 \), \( \mathbb{F}_r \subset L \), and \( a_i \notin L \) for all \( 1 \leq i \leq l \). Let \( H \) be an \( \mathbb{F}_r \)-subspace of \( L \) such that \( \mathbb{F}_r \subset H \) and \( \dim_{\mathbb{F}_r} H = d \). For each \( 1 \leq i \leq l \), since \( 1 \in H \) and \( a_i \notin H \), we have \( \mathbb{F}_{r^i} \nsubseteq H \). Hence \( H^\dagger = \mathbb{F}_r \). \( \Box \)

The input data for (4.15) and (4.27) are \( p, \alpha, k, d, i, j \), where \( 0 \leq k \leq p^\alpha / 2, d \mid p^\alpha - 1, i \mid (\alpha / o_d(p)), j = 0 \) if \( i = \alpha / o_d(p) \), and \( 0 < j < \alpha / o_d(p) \) if \( i < \alpha / o_d(p), k \equiv 0 \) or \( p^\alpha (p) \). These data produce \( q = p^\alpha, |H| = p^\beta \), where \( \beta = o_d(p) i j \), and \( |H^\dagger| = p^\beta (p) i j \). Afterwards, \( \mathcal{N}(\mathbb{F}_q^i / \mathbb{F}_q, 0, H, k) \) can be computed (with computer assistance) by (4.15) (for \( d = 1 \)) and by (4.27) (for \( d > 1 \)). A Mathematica code is included in Appendix A1; the computational results for \( q \leq 16 \) are given in Table 1 in Appendix A2. An extended table of values of \( \mathcal{N}(\mathbb{F}_q^i / \mathbb{F}_q, 0, H, k) \) with \( q \leq 101 \) is available in [8].

6 Remarks and open questions

Let \( S_q \) denote the set of all subgroups of \( \text{AGL}(1, \mathbb{F}_q) \). Fix \( 0 \leq k \leq q \). There are two maps between \( S_q \) and \( (\mathbb{F}_q^k) \):

\[
(\gamma) : S_q \longrightarrow (\mathbb{F}_q^k)
\]

\[ S \longmapsto S' = \left\{ B \in (\mathbb{F}_q^k) : \sigma(B) = B \text{ for all } \sigma \in S \right\}, \tag{6.1}
\]

and

\[
(\gamma) : (\mathbb{F}_q^k) \longrightarrow S_q
\]

\[ B \longmapsto B' = \text{AGL}(1, \mathbb{F}_q)_B. \tag{6.2}
\]

These two maps enjoy the properties of a “Galois correspondence”: both \( (\gamma) \) are inclusion reversing; \( S \subset S'' \) and \( B \subset B'' \) for all \( S \in S_q \) and \( B \in (\mathbb{F}_q^k) \); \( (\gamma)'' = (\gamma) \). The map \( (\gamma) : S_q \rightarrow (\mathbb{F}_q^k) \) has been described in Sect. 3.3. However, the map \( (\gamma) : (\mathbb{F}_q^k) \rightarrow S_q \) is not well understood; in particular, Question 1.3 asks about the image of this map.

Theorems 4.2 and 4.4 show that one can “compute” an answer to Question 1.3 (for \( \text{AGL}(1, \mathbb{F}_q) \)) by computing the function \( \mathcal{N} = \mathcal{N}(\gamma(q^{-1}) / d, 0, H, k) \). We do not know if it is possible to find a more theoretic and general solution to Question 1.3 for \( \text{AGL}(1, \mathbb{F}_q) \).

Sun [16] gave several constructions of \( B \in (\mathbb{F}_q^k) \) with specified stabilizers. Those results can be stated in terms of the nonvanishingness of the function \( \mathcal{N} \) as follows:

**Theorem 6.1** ([16, Theorem 4.14], Lemma 5.1) Let \( H < \mathbb{F}_q \) with \( H^\dagger = \mathbb{F}_p^i \). Then

\[ \text{AGL}(1, \mathbb{F}_q)_H = \mathcal{N}(\gamma(q^{-1}) / (p^i - 1), 0, H). \]

In particular, for \( (\beta, i) = (0, \alpha) \) or \( (\alpha, \alpha) \), or \( 0 < \beta < \alpha \) and \( i \mid \gcd(\alpha, \beta) \), there exists \( H < \mathbb{F}_q \) with \( |H| = p^\beta \) and \( |H^\dagger| = p^i \) such that

\[ \mathcal{N}(\gamma(q^{-1}) / (p^i - 1), 0, H, p^\beta) > 0. \]
Theorem 6.2 [16, Theorem 3.5] Assume that $3 \leq k \leq q/2$, $p \nmid k$, $d \mid q - 1$, $k \equiv 0 \text{ or } 1 \pmod{d}$, and $(q, k, d) \neq (7, 3, 1)$. Then

$$\mathcal{N}(S(y^{(q-1)/d}, 0, \{0\}), k) > 0.$$ 

Theorem 6.3 [16, Theorem 4.4] Assume that $3 \leq k \leq q/2$ and

$$k \equiv \begin{cases} 2 \pmod{4} & \text{if } p = 2, \\ 0 \pmod{p} & \text{if } p > 2. \end{cases}$$

Then

$$\mathcal{N}(S(1, 0, \{0\}), k) > 0.$$

(This corresponds to $d = 1$ and $\beta = 0$ in (A1.1).)

Theorem 6.4 [16, Theorem 4.17] Let $\beta, d, m$ be positive integers such that $\beta \mid \alpha$, $\beta < \alpha$, $p^\beta > 2$ and $d + m \leq \alpha/\beta$. Let $c_1, k_1 (1 \leq i \leq m)$ be positive integers such that $c_i \mid p^\beta - 1$, $\gcd(c_1, \ldots, c_m) = c > 1$, and $p \nmid k_i$. Further assume that for each $1 \leq i \leq m$, $c_i \mid k_i$ and $2 \leq k_i \leq p^\beta - 3$, or $c_i \mid k_i - 1$ and $3 \leq k_i \leq p^\beta - 2$. Then

$$\mathcal{N}(S(y^{(q-1)/c}, 0, H), k_1 \cdots k_m p^{\beta d}) > 0$$

for some $H < \mathbb{F}_q$ with $|H| = p^{\beta d}$ and $|H^\alpha| = p^{\beta}$.

Our numerical results are consistent with the above theorems. Moreover, the numerical results in Appendix A2 and in [8] provide plenty material for conjectures and open questions about the function $\mathcal{N}(S(S^{(q-1)/d}, 0, H), k)$. We include a few open questions to invite further work. We always assume that $k \equiv 0$ or $|H| \pmod{d|H|})$, which is necessary for $\mathcal{N} \neq 0$ (Remark 4.6 (i)).

Question 6.5 For $3 \leq k \leq q/2$, $\mathcal{N} = 0$ only if $p \mid k$ (Theorem 6.2). Determine exactly when $\mathcal{N} = 0$.

Question 6.6 (A subquestion of Question 6.5) For $p = 2$ and $3 \leq k \leq q/2$, it appears that $\mathcal{N} = 0$ only if $k$ is a power of 2. Is this true?

Question 6.7 In certain cases where $\mathcal{N}(S, k)$ is positive but small, determine those $B \in (\mathbb{F}_q^k)$ such that $AGL(1, \mathbb{F}_q)_B = S$.

Question 6.8 Determine the $p$-adic valuation of $\mathcal{N}(S, k)$ in (4.15) and (4.27). This could give $\mathcal{N}(S, k) \neq 0$ without computations involving large integers.

The work of the present paper relies on a fairly detailed description of the lattice of subgroups of $AGL(1, \mathbb{F}_q)$. In fact, based on the approach of the present paper, we are able to determine the Möbius function of the lattice of subgroups of $AGL(1, \mathbb{F}_q)$ [9].

Appendix

A1. A Mathematica code for computing $\mathcal{N}(S(y^{(q-1)/d}, 0, H), k)$
In the following Mathematica program, the input is \( q = p^\alpha \); the output is the array \((k, d, o_d(p), i, j, \beta, N)\), where
\[
0 \leq k \leq p^{\alpha}/2, \\
\begin{align*}
d &\mid p^\alpha - 1, \\
i &\mid (\alpha/o_d(p)),
\end{align*}
\]
\[
\begin{cases} 
  j = 0, 1 & \text{if } i = \alpha/o_d(p), \\
  0 < j < \alpha/o_d(p)i & \text{if } i < \alpha/o_d(p),
\end{cases}
\]
\( \beta = o_d(\alpha)ij, \)
\( k \equiv 0 \text{ or } p^\beta \pmod{dp^\beta}, \)
\( N = N'(\gamma^{(q-1)/d}, 0, H, k), \)
where \(|H| = p^\beta, |H^*| = p^{o_d(p)i} \).

\begin{verbatim}
In[1] :=

MyBinom[x_, y_] := If[IntegerQ[y], Binomial[x, y], 0];
s[q_, k_, x_, y_] := MyBinom[(q - y)/(x*y), k/(x*y)] + MyBinom[(q - y)/(x*y), (k - y)/(x*y)];

p = 2;
alpha = 4;
q = p^alpha;
Print["q = ", p, "^", alpha];
divd = Sort[Divisors[q - 1]]; 
For[k = 0, k <= q/2, k++,
  For[u = 1, u <= Length[divd], u++,
    d = Extract[divd, {u}];
    odp = MultiplicativeOrder[p, d];
    divi = Sort[Divisors[alpha/odp]];
    For[v = 1, v <= Length[divi], v++,
      i = Extract[divi, {v}];
      If[i == alpha/odp, j0 = 0; j1 = 1; j0 = 1; j1 = alpha/(odp*i) - 1];
      For[j = j0, j <= j1, j++,
        beta = odp*i*j;
        condition = Mod[k, d*p^beta];
        If[condition != 0 \&\& condition != p^beta, Continue[]];
        x = (p^(odp*i) - 1)/d;
        If[x == 1, PSet = {},
          PSet = FactorInteger[x][[All, 1]]];
        PP = Subsets[PSet];
        If[d == 1,
          Num = (1 - p^(alpha - beta))*
            Sum[(-1)^l*p^Binomial[l, 2]*QBinomial[alpha - beta, 1, p]*
              s[q, k, l, p^(beta + l)], {l, 0, alpha - beta}],
          Num = 0];
        N1 = 0;
        For[t = 1, t <= Length[PP], t++,
          P = Extract[PP, {t}];
          piP = Times @@ P;
          
```
A2. Numerical results

Table 1 gives the values of $\mathcal{N}(S(\gamma^{(q-1)/d}, 0, H), k)$ for $q \leq 16$. To recall the meanings of and the conditions on the parameters, refer to (A1.1) in Appendix A1.

| $p$ | $\alpha$ | $k$ | $d$ | $o_d(p)$ | $i$ | $j$ | $\beta$ | $\mathcal{N}$ |
|-----|----------|-----|-----|---------|-----|-----|---------|-------------|
| 2   | 1        | 0   | 1   | 1       | 1   | 0   | 0       | 0           |
|     |          | 0   | 1   | 1       | 1   | 1   | 1       | 1           |
|     |          | 1   | 1   | 1       | 0   | 1   | 0       | 2           |
| 2   | 2        | 0   | 1   | 1       | 1   | 1   | 0       | 0           |
|     |          | 0   | 1   | 2       | 0   | 0   | 0       | 0           |
|     |          | 0   | 1   | 2       | 1   | 2   | 0       | 0           |
|     |          | 0   | 3   | 2       | 1   | 0   | 0       | 0           |
|     |          | 0   | 3   | 2       | 1   | 1   | 2       | 1           |
|     |          | 1   | 1   | 1       | 2   | 0   | 0       | 0           |
|     |          | 1   | 3   | 2       | 1   | 0   | 0       | 1           |
|     |          | 2   | 1   | 1       | 1   | 1   | 2       | 1           |
|     |          | 2   | 1   | 2       | 0   | 0   | 0       | 0           |
| 2   | 3        | 0   | 1   | 1       | 1   | 1   | 1       | 0           |
|     |          | 0   | 1   | 2       | 2   | 0   | 0       | 0           |
|     |          | 0   | 1   | 3       | 0   | 0   | 0       | 0           |
|     |          | 0   | 1   | 3       | 1   | 3   | 0       | 0           |
|     |          | 0   | 7   | 3       | 1   | 0   | 0       | 0           |
|     |          | 0   | 7   | 3       | 1   | 1   | 3       | 1           |
|     |          | 1   | 1   | 3       | 0   | 0   | 0       | 0           |
|     |          | 1   | 7   | 3       | 1   | 0   | 0       | 1           |
|     |          | 2   | 1   | 1       | 2   | 0   | 0       | 0           |
|     |          | 2   | 1   | 1       | 1   | 1   | 1       | 0           |
|     |          | 2   | 1   | 3       | 0   | 0   | 0       | 0           |
| p | α | k | d | α_d(p) | i | j | β | N  |
|---|---|---|---|---------|---|---|---|----|
| 3 | 1 | 1 | 1 | 3 | 0 | 0 | 0 | 56 |
| 4 | 1 | 1 | 1 | 1 | 1 | 1 | 0 |    |
| 4 | 1 | 1 | 1 | 2 | 2 | 2 |    |    |
| 4 | 1 | 1 | 3 | 0 | 0 | 0 | 56 |    |
| 2 | 4 | 0 | 1 | 1 | 1 | 1 | 1 | 0  |
|    | 0 | 1 | 1 | 1 | 2 | 2 | 0 |    |
|    | 0 | 1 | 1 | 1 | 3 | 3 | 0 |    |
|    | 0 | 1 | 1 | 2 | 1 | 2 | 0 |    |
|    | 0 | 1 | 1 | 4 | 0 | 0 | 0 |    |
|    | 0 | 1 | 1 | 4 | 1 | 4 | 0 |    |
|    | 0 | 3 | 2 | 1 | 1 | 2 | 0 |    |
|    | 0 | 3 | 2 | 2 | 0 | 0 | 0 |    |
|    | 0 | 3 | 2 | 2 | 1 | 4 | 0 |    |
|    | 0 | 5 | 4 | 1 | 0 | 0 | 0 |    |
|    | 0 | 5 | 4 | 1 | 1 | 4 | 0 |    |
|    | 0 | 15 | 4 | 1 | 0 | 0 | 0 |    |
|    | 0 | 15 | 4 | 1 | 1 | 4 | 1 |    |
|    | 1 | 1 | 4 | 0 | 0 | 0 |    |    |
|    | 1 | 3 | 2 | 2 | 0 | 0 | 0 |    |
|    | 1 | 5 | 4 | 1 | 0 | 0 | 0 |    |
|    | 1 | 15 | 4 | 1 | 0 | 0 | 1 |    |
| 2 | 4 | 2 | 1 | 1 | 1 | 1 | 1 | 8  |
|    | 2 | 1 | 1 | 4 | 0 | 0 | 0 |    |
|    | 3 | 1 | 1 | 4 | 0 | 0 | 480|    |
|    | 3 | 3 | 2 | 2 | 0 | 0 | 5  |    |
|    | 4 | 1 | 1 | 1 | 1 | 1 | 0  |    |
|    | 4 | 1 | 1 | 1 | 2 | 2 | 4  |    |
|    | 4 | 1 | 1 | 2 | 1 | 2 | 0  |    |
|    | 4 | 1 | 1 | 4 | 0 | 0 | 1680|    |
|    | 4 | 3 | 2 | 1 | 1 | 2 | 1  |    |
|    | 4 | 3 | 2 | 2 | 0 | 0 | 0  |    |
|    | 5 | 1 | 1 | 4 | 0 | 0 | 4320|    |
|    | 5 | 5 | 4 | 1 | 0 | 0 | 3  |    |
|    | 6 | 1 | 1 | 1 | 1 | 1 | 56 |    |
|    | 6 | 1 | 1 | 4 | 0 | 0 | 6960|    |
|    | 6 | 3 | 2 | 2 | 0 | 0 | 10 |    |
|    | 6 | 5 | 4 | 1 | 0 | 0 | 3  |    |
|    | 7 | 1 | 1 | 4 | 0 | 0 | 11280|    |
|    | 7 | 3 | 2 | 2 | 0 | 0 | 10 |    |
|    | 8 | 1 | 1 | 1 | 1 | 1 | 56 |    |
| $p$ | $\alpha$ | $k$ | $d$ | $\alpha_d(p)$ | $i$ | $j$ | $\beta$ | $N$ |
|-----|----------|-----|-----|---------------|-----|-----|---------|-----|
| 8   | 1        | 1   | 1   | 2             | 2   | 0   |         |     |
| 8   | 1        | 1   | 1   | 3             | 3   | 2   |         |     |
| 8   | 1        | 1   | 2   | 1             | 2   | 0   |         |     |
| 8   | 1        | 1   | 4   | 0             | 0   | 0   | 12000   |     |
| 3   | 1        | 0   | 1   | 1             | 0   | 0   | 0       |     |
|     | 0        | 1   | 1   | 1             | 1   | 0   |         |     |
|     | 0        | 2   | 1   | 1             | 0   | 0   | 0       |     |
|     | 0        | 2   | 1   | 1             | 1   | 1   |         |     |
|     | 1        | 1   | 1   | 1             | 0   | 0   | 0       |     |
|     | 1        | 2   | 1   | 1             | 0   | 0   | 1       |     |
| 3   | 2        | 0   | 1   | 1             | 1   | 1   | 1       |     |
|     | 0        | 1   | 1   | 2             | 0   | 0   | 0       |     |
|     | 0        | 1   | 1   | 2             | 1   | 2   | 0       |     |
|     | 0        | 2   | 1   | 1             | 1   | 1   | 0       |     |
|     | 0        | 2   | 1   | 2             | 0   | 0   | 0       |     |
|     | 0        | 2   | 1   | 2             | 1   | 2   | 0       |     |
|     | 0        | 4   | 2   | 1             | 0   | 0   | 0       |     |
|     | 0        | 4   | 2   | 1             | 1   | 2   | 0       |     |
|     | 0        | 8   | 2   | 1             | 0   | 0   | 0       |     |
|     | 0        | 8   | 2   | 1             | 1   | 2   | 1       |     |
|     | 1        | 1   | 1   | 2             | 0   | 0   | 0       |     |
|     | 1        | 2   | 1   | 2             | 0   | 0   | 0       |     |
|     | 1        | 4   | 2   | 1             | 0   | 0   | 0       |     |
|     | 1        | 8   | 2   | 1             | 0   | 0   | 1       |     |
|     | 2        | 1   | 1   | 2             | 0   | 0   | 0       |     |
|     | 2        | 2   | 1   | 2             | 0   | 0   | 4       |     |
| 3   | 2        | 3   | 1   | 1             | 1   | 1   | 1       |     |
|     | 3        | 1   | 1   | 2             | 0   | 0   | 72      |     |
|     | 3        | 2   | 1   | 1             | 1   | 1   | 1       |     |
|     | 3        | 2   | 1   | 2             | 0   | 0   | 0       |     |
|     | 4        | 1   | 1   | 2             | 0   | 0   | 72      |     |
|     | 4        | 2   | 1   | 2             | 0   | 0   | 4       |     |
|     | 4        | 4   | 2   | 1             | 0   | 0   | 2       |     |
| 5   | 1        | 0   | 1   | 1             | 0   | 0   | 0       |     |
|     | 0        | 1   | 1   | 1             | 1   | 1   | 0       |     |
|     | 0        | 2   | 1   | 1             | 0   | 0   | 0       |     |
|     | 0        | 2   | 1   | 1             | 1   | 1   | 0       |     |
|     | 0        | 4   | 1   | 1             | 0   | 0   | 0       |     |
|     | 0        | 4   | 1   | 1             | 1   | 1   | 1       |     |
|     | 1        | 1   | 1   | 1             | 0   | 0   | 0       |     |
|     | 1        | 2   | 1   | 1             | 0   | 0   | 0       |     |
Table 1 continued

| $p$ | $\alpha$ | $k$ | $d$ | $o_d(p)$ | $i$ | $j$ | $\beta$ | $N$ |
|-----|----------|-----|-----|----------|-----|-----|---------|-----|
| 1   | 4        | 1   | 1   | 1        | 0   | 0   | 1       |     |
| 2   | 1        | 1   | 1   | 1        | 0   | 0   | 0       |     |
| 2   | 2        | 1   | 1   | 1        | 0   | 0   | 2       |     |
| 7   | 1        | 0   | 1   | 1        | 1   | 0   | 0       |     |
|     | 0        | 1   | 1   | 1        | 1   | 1   | 0       |     |
|     | 0        | 2   | 1   | 1        | 0   | 0   | 0       |     |
|     | 0        | 2   | 1   | 1        | 1   | 1   | 0       |     |
|     | 0        | 3   | 1   | 1        | 0   | 0   | 0       |     |
|     | 0        | 3   | 1   | 1        | 1   | 1   | 0       |     |
|     | 0        | 6   | 1   | 1        | 0   | 0   | 0       |     |
|     | 0        | 6   | 1   | 1        | 1   | 1   | 1       |     |
|     | 1        | 1   | 1   | 1        | 0   | 0   | 0       |     |
|     | 1        | 2   | 1   | 1        | 0   | 0   | 0       |     |
|     | 1        | 3   | 1   | 1        | 0   | 0   | 0       |     |
|     | 1        | 6   | 1   | 1        | 0   | 0   | 1       |     |
|     | 2        | 1   | 1   | 1        | 0   | 0   | 0       |     |
|     | 2        | 2   | 1   | 1        | 0   | 0   | 3       |     |
|     | 3        | 1   | 1   | 1        | 0   | 0   | 0       |     |
|     | 3        | 2   | 1   | 1        | 0   | 0   | 3       |     |
| 11  | 1        | 0   | 1   | 1        | 0   | 0   | 0       |     |
|     | 0        | 1   | 1   | 1        | 1   | 1   | 0       |     |
|     | 0        | 2   | 1   | 1        | 0   | 0   | 0       |     |
|     | 0        | 2   | 1   | 1        | 1   | 1   | 0       |     |
|     | 0        | 5   | 1   | 1        | 0   | 0   | 0       |     |
|     | 0        | 5   | 1   | 1        | 1   | 1   | 0       |     |
|     | 0        | 10  | 1   | 1        | 0   | 0   | 0       |     |
|     | 0        | 10  | 1   | 1        | 1   | 1   | 1       |     |
|     | 1        | 1   | 1   | 1        | 0   | 0   | 0       |     |
|     | 1        | 2   | 1   | 1        | 0   | 0   | 0       |     |
|     | 1        | 5   | 1   | 1        | 0   | 0   | 0       |     |
|     | 1        | 10  | 1   | 1        | 0   | 0   | 1       |     |
| 11  | 1        | 2   | 1   | 1        | 0   | 0   | 0       |     |
| 2   | 2        | 1   | 1   | 1        | 0   | 0   | 5       |     |
| 3   | 1        | 1   | 1   | 1        | 0   | 0   | 110     |     |
| 3   | 2        | 1   | 1   | 1        | 0   | 0   | 5       |     |
| 4   | 1        | 1   | 1   | 1        | 0   | 0   | 220     |     |
| 4   | 2        | 1   | 1   | 1        | 0   | 0   | 10      |     |
| 5   | 1        | 1   | 1   | 1        | 0   | 0   | 330     |     |
| 5   | 2        | 1   | 1   | 1        | 0   | 0   | 10      |     |
| 5   | 5        | 1   | 1   | 1        | 0   | 0   | 2       |     |
Table 1  continued

| $p$ | $\alpha$ | $k$ | $d$ | $o_d(p)$ | $i$ | $j$ | $\beta$ | $N$ |
|-----|----------|-----|-----|-----------|-----|-----|---------|-----|
| 13  | 1        | 0   | 1   | 1         | 1   | 0   | 0       | 0   |
|     | 0        | 1   | 1   | 1         | 1   | 1   | 1       | 0   |
|     | 0        | 2   | 1   | 1         | 0   | 0   | 0       | 0   |
|     | 0        | 2   | 1   | 1         | 1   | 1   | 1       | 0   |
|     | 0        | 3   | 1   | 1         | 0   | 0   | 0       | 0   |
|     | 0        | 3   | 1   | 1         | 1   | 1   | 1       | 0   |
|     | 0        | 4   | 1   | 1         | 0   | 0   | 0       | 0   |
|     | 0        | 4   | 1   | 1         | 1   | 1   | 1       | 0   |
|     | 0        | 6   | 1   | 1         | 0   | 0   | 0       | 0   |
|     | 0        | 6   | 1   | 1         | 1   | 1   | 1       | 0   |
|     | 0        | 12  | 1   | 1         | 0   | 0   | 0       | 0   |
|     | 0       | 12  | 1   | 1         | 1   | 1   | 1       | 1   |
|     | 1       | 1   | 1   | 1         | 0   | 0   | 0       | 0   |
|     | 1       | 2   | 1   | 1         | 0   | 0   | 0       | 0   |
|     | 1       | 3   | 1   | 1         | 0   | 0   | 0       | 0   |
|     | 1       | 4   | 1   | 1         | 0   | 0   | 0       | 0   |
|     | 1       | 6   | 1   | 1         | 0   | 0   | 0       | 0   |
|     | 1       | 12  | 1   | 1         | 0   | 0   | 1       | 1   |
|     | 2       | 1   | 1   | 1         | 0   | 0   | 0       | 0   |
|     | 2       | 2   | 1   | 1         | 0   | 0   | 6       | 6   |
|     | 3       | 1   | 1   | 1         | 0   | 0   | 156     | 156 |
|     | 3       | 2   | 1   | 1         | 0   | 0   | 6       | 6   |
|     | 3       | 3   | 1   | 1         | 0   | 0   | 4       | 4   |
|     | 4       | 1   | 1   | 1         | 0   | 0   | 468     | 468 |
|     | 4       | 2   | 1   | 1         | 0   | 0   | 12      | 12  |
|     | 4       | 3   | 1   | 1         | 0   | 0   | 4       | 4   |
|     | 4       | 4   | 1   | 1         | 0   | 0   | 3       | 3   |
|     | 5       | 1   | 1   | 1         | 0   | 0   | 1092    | 1092|
|     | 5       | 2   | 1   | 1         | 0   | 0   | 12      | 12  |
|     | 5       | 4   | 1   | 1         | 0   | 0   | 3       | 3   |
|     | 6       | 1   | 1   | 1         | 0   | 0   | 1404    | 1404|
|     | 6       | 2   | 1   | 1         | 0   | 0   | 18      | 18  |
|     | 6       | 3   | 1   | 1         | 0   | 0   | 4       | 4   |
|     | 6       | 6   | 1   | 1         | 0   | 0   | 2       | 2   |

References

1. Agrell E., Vardy A., Zeger K.: Upper bounds for constant-weight codes. IEEE Trans. Inf. Theory 46, 2373–2395 (2000).
2. Bender E.A., Goldman J.R.: On the applications Möbius inversion in combinatorial analysis. Am. Math. Mon. 82, 789–803 (1975).
3. Brouwer A.E., Etzion T.: Some new distance-4 constant weight codes. Adv. Math. Commun. 5, 417–424 (2011).
4. Brouwer A.E., Shearer J.B., Sloane N.J.A., Smith W.D.: A new table of constant weight codes. IEEE Trans. Inf. Theory 36, 1334–1380 (1990).
5. Cameron P.J., Maimani H.R., Omidi G.R., Tayfeh-Rezaie B.: 3-Designs from PSL(2, q). Discret. Math. 306, 3063–3073 (2006).
6. Cameron P.J., Omidi G.R., Tayfeh-Rezaie B.: 3-Designs from PGL(2, q). Electron. J. Comb. 13, R50 (2006).
7. Chee Y.M., Xing C., Yeo S.L.: New constant-weight codes from propagation rules. IEEE Trans. Inf. Theory 56, 1596–1599 (2010).
8. Hou X.: Optimal binary constant weight codes and affine groups over finite fields. arXiv:1707.02315.
9. Hou X.: The Möbius function of the affine linear AGL(1, q), preprint.
10. Huffman W.C., Pless V.: Fundamentals of Error-Correcting Codes. Cambridge University Press, Cambridge, UK (2003).
11. Johnson S.M.: A new bound for error-correcting codes. IEEE Trans. Inf. Theory 8, 203–207 (1962).
12. Östergård P.R.J.: Classification of binary constant weight codes. IEEE Trans. Inf. Theory 56, 3779–3785 (2010).
13. Schrijver A.: New code upper bounds from the Terwilliger algebra and semidefinite programming. IEEE Trans. Inf. Theory 51, 2859–2866 (2005).
14. Semakov N.V., Zinov’ev V.A.: Balanced codes and tactical configurations. Probl. Inf. Transm. 5, 22–28 (1969).
15. Smith D.H., Hughes L.A., Perkins S.: A new table of constant weight codes of length greater than 28. Electron. J. Comb. 13 Article 2 (2006).
16. Sun H.-M.: From planar nearrings to generating blocks. Taiwan. J. Math. 14, 1713–1739 (2010).
17. Sun H.-M.: Some sequences of optimal constant weight codes. J. Alg. Appl. 17, 1850027 (2018).
18. Tonchev V.D.: Combinatorial Configurations. Longman-Wiley, New York (1988).

Publisher’s Note Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.