Minimal blocks of points with weight divisible by $p$ over GF($p$)

Joseph P.S. Kung

Department of Mathematics, University of North Texas, Denton, TX 76203, USA

1. Minimal blocks

A $k$-block $M$ over the finite field GF($q$) can be defined as a set of points in a projective space PG($n-1, q$) over GF($q$) such that every codimension-$k$ subspace in PG($n-1, q$) contains at least one point in $M$. Equivalently, $M$ is a $k$-block if for any system of $k$ homogeneous linear equations

$$a_{j_1}x_1 + a_{j_2}x_2 + \cdots + a_{j_k}x_n = 0, \quad 1 \leq j \leq k,$$

there is a (nonzero) solution lying in $M$. The $k$-block $M$ is minimal if for every point $z$ in $M$, there exists at least one codimension-$k$ subspace $U$ in PG($n-1, q$) such that $U \cap M = \{z\}$. Such a subspace is called a tangent of $z$. The theory of minimal blocks was initiated by Tutte in [7], in 1966. Brief
accounts of the theory of minimal blocks (in particular, the fact that for a given \( q \), being a minimal block over \( \text{GF}(q) \) depends only on the matroid structure) can be found in [5,6].

Let \( q \) be a prime power and \( e_1, e_2, \ldots, e_n \) be a chosen basis of \( \text{PG}(n-1, q) \). Let \( z \) be a point in \( \text{PG}(n-1, q) \). Then up to a nonzero factor, \( z \) can be expressed uniquely as a nonzero linear combination
\[
z = \sum_{i=1}^{n} z_i e_i \quad \text{or} \quad z = (z_1, z_2, \ldots, z_n).
\]
Its support \( \text{supp}(z) \) (relative to the chosen basis) is the set \( \{i \mid z_i \neq 0\} \) and its \text{(Hamming) weight} \( |z| \) is the size of its support. As the origin is deleted when constructing a projective geometry, points always have positive weight. If \( I \subseteq \{1, 2, \ldots, n\} \), let
\[
e[I] = \sum_{i \in I} e_i.
\]
Let \( \alpha \) divide \( q-1 \) and \( B(q; n, s, \alpha) \) be the set of points \( z \) in \( \text{PG}(n-1, q) \) such that \( |z| = s \) and there exists a nonzero element \( \alpha \in \text{GF}(q) \) such that every nonzero coordinate in \( (az_1, az_2, \ldots, az_n) \) satisfies the condition \((az_i)\alpha = 1\), or equivalently, \( az_i \) has order dividing \( \alpha \) in the multiplicative group \( \text{GF}(q)\times \). For example, since the only element in \( \text{GF}(q)\times \) of order 1 is the identity 1,
\[
B(q; n, s, 1) = \{e[I] : |I| = s\},
\]
the set of points with exactly \( s \) coordinates equal to 1 and the other coordinates equal to 0. At the other extreme, by Fermat’s little theorem for finite fields, every element has order dividing \( q-1 \). Hence,
\[
B(q; n, s, q-1) = \{z : \text{weight}(z) = s\},
\]
the set of all points having weight exactly \( s \). For an example of a set in the middle, let \( q \) be odd. Then \( B(q; n, s, 2) \) is the set of points expressible as a vector \( u \) such that \( \text{weight}(u) = s \) and the nonzero coordinates in \( u \) equal 1 or \(-1\). We are also interested in unions of \( B(p; n, s, \alpha) \). Let
\[
\bar{B}(p; n, \alpha) = \bigcup_{i=1}^{[n/p]} B(p; n, ip, \alpha);
\]
that is, \( \bar{B}(p; n, \alpha) \) is the set of points \( \text{PG}(n-1, p) \) satisfying the same order condition on its nonzero coordinates as \( B(p; n, s, \alpha) \) with weight not equal to 0 and divisible by \( p \).

We will prove the following theorems.

**Theorem 1.1.** Let \( p \) be a prime and \( m \) be a positive integer. If \( n \geq p + m(p-1)/\alpha \), then \( \bar{B}(p; n, \alpha) \) is an \( m \)-block. In particular, \( B(p; 2p-1, p, \alpha) \) is an \( \alpha \)-block and \( \bar{B}(p; \gamma p-1, p-1) \) is a \((\gamma-1)p-1\)-block.

**Theorem 1.2.** Let \( p \) be an odd prime. Then

(a) \( B(p; 2p-1, p, 1) \) is a minimal 1-block,

(b) \( B(p; 2p-1, p, 2) \) is a minimal 2-block,

(c) \( \bar{B}(p; \gamma p-1, p-1) \) is a minimal \((\gamma-1)p-1\)-block.

Since \( B(p; 2p-1, p, 1) \) is contained in the codimension-1 subspace or hyperplane defined by the equation \( x_1 + x_2 + \cdots + x_{2p-1} = 0 \), it does not span \( \text{PG}(2p-2, p) \). It is easy to show that \( B(p; 2p-1, p, 1) \) has rank \( 2p-2 \). The other two blocks, \( B(p; 2p-1, p, 2) \) and \( \bar{B}(p; \gamma p-1, p-1) \), span their ambient projective space when \( p \) is odd. Note that \( B(2; 3, 2, 1) = \{(1, 1, 0), (1, 0, 1), (0, 1, 1)\} \) and its matroid is \( U_{2,3} \), the 3-point line. Hence, \( B(2; 3, 2, 1) \) is a tangential 1-block over \( \text{GF}(2) \). Results for finite fields of characteristic 2 similar to those in this paper have appeared in [6].
2. Solving polynomial equations over finite fields

To prove Theorem 1.1, we will use the Chevalley–Warning theorem [2,8] from number theory. This theorem is elementary and an accessible self-contained exposition of this theorem can be found in [4], p. 143.

The Chevalley–Warning theorem. For $1 \leq i \leq t$, let $f_i(x_1, x_2, \ldots, x_n)$ be a polynomial in $n$ variables of total degree $d_i$, with no constant term, having coefficients in the finite field $\text{GF}(q)$. If $n > \sum_{i=1}^{t} d_i$, then the polynomial equations $f_1 = 0, f_2 = 0, \ldots, f_t = 0$ have at least two common solutions over $\text{GF}(q)^n$. In particular, the polynomial equations have a common solution not equal to the origin.

Proof of Theorem 1.1. We begin with a lemma.

Lemma 2.1. Let $\alpha$ divide $p - 1$ and $[a_{ji}]_{1 \leq j \leq m, 1 \leq i \leq n}$ be an $m \times n$ matrix over $\text{GF}(p)$. If the polynomial equations

$$a_{j1}x_1^{(p-1)/\alpha} + a_{j2}x_2^{(p-1)/\alpha} + \cdots + a_{jn}x_n^{(p-1)/\alpha} = 0, \quad 1 \leq j \leq m, \quad (2.1)$$

and

$$x_1^{p-1} + x_2^{p-1} + \cdots + x_n^{p-1} = 0 \quad (2.2)$$

have a common nonzero solution $(z_1, z_2, \ldots, z_n)$ in $\text{GF}(p)^n$, then the system of linear equations

$$a_{j1}x_1 + a_{j2}x_2 + \cdots + a_{jn}x_n = 0, \quad 1 \leq j \leq m. \quad (2.3)$$

has a nonzero solution $(z'_1, z'_2, \ldots, z'_n)$ in $\text{GF}(p)^n$ with weight congruent to 0 modulo $p$ and each nonzero coordinate $z'_i$ having order dividing $\alpha$ in $\text{GF}(p)^x$.

Proof. Let $z = (z_1, z_2, \ldots, z_n)$ and $z' = (z'_1/\alpha, z'_2/\alpha, \ldots, z'_n/\alpha)$. Note that $z$ and $z'$ have the same support. Suppose that $z$ is a nonzero common solution of the polynomial Eqs. (2.1). Then $z'$ is a nonzero solution of the system (2.3) of linear equations. Since $z$ is a nonzero solution of Eq. (2.2) and $x_i^{p-1}$ equals 1 when $z_i \neq 0$ and 0 if $z_i = 0$, $(z_1^{p-1}, z_2^{p-1}, \ldots, z_n^{p-1})$ is a solution with coordinates equal to 0 or 1 of the equation

$$x_1 + x_2 + \cdots + x_n = 0.$$

The only such solutions are $e[I]$, where $I = \text{supp}(z)$ and $|I| \equiv 0 \mod p$. Since $\text{supp}(z') = \text{supp}(z)$, we conclude that

$$|\text{supp}(z')| = |I| \equiv 0 \mod p.$$

To finish the proof, observe that if $z_i \neq 0$, then $(z_i^{(p-1)/\alpha})^\alpha = z_i^{p-1} = 1$. Hence, every nonzero coordinate $z'_i$ in $z$ satisfies $(z'_i)^\alpha = 1$. □

Returning to the proof of Theorem 1.1, let $n > m(p - 1)/\alpha + p - 1$. Then the Chevalley–Warning theorem implies that there exists a nonzero solution of the polynomial equations, and hence, a solution in $B(p; n, \alpha)$ of the system (2.3) of linear equations. We conclude that $B(p; n, \alpha)$ is an $m$-block. □
Proof of Theorem 1.2. We construct a tangent for each point in the 1-block $B(p; 2p - 1, p, 1)$. Let $I \subseteq \{1, 2, \ldots, 2p - 1\}$ and $|I| = p$. Consider the hyperplane $H$ defined by the linear equation

$$\sum_{i \in I} x_i = 0. \quad (2.4)$$

Since $e[I]$ is a solution of Eq. (2.4), $e[I] \in H$. To finish, suppose that $e[J]$ is another point in $B(p; 2p - 1, p, 1)$. Then $|J| = p$, $J \neq I$, and hence, $1 \leq |I \cap J| \leq p - 1$. In particular, $e[J]$ is not a solution to Eq. (2.4) and $e[J] \notin H$.

Next, we prove (b) by constructing a tangent for each point $z$ in the 2-block $B(p; 2p - 1, p, 2)$. The points in this block have $p$ nonzero coordinates equal to 1 or $-1$, and $p - 1$ coordinates equal to 0's. Since $B(p; 2p - 1, p, 2)$ is invariant under a permutation of coordinates, we may assume that $z$ has the form

$$(1, 1, \ldots, 1, -1, -1, \ldots, -1, 0, 0, \ldots, 0),$$

where there are $c$ 1's, $d$ $-1$'s, and $c + d = p$. Consider the codimension-2 subspace $U$ defined by the two linear equations

$$\left( \sum_{i=1}^{c} x_i \right) - \left( \sum_{i=c+1}^{p} x_i \right) = 0 \quad (2.5)$$

and

$$\sum_{i=p+1}^{2p-1} x_i = 0. \quad (2.6)$$

Then $z \in U$. Suppose that $y$ is another point in $B(p; 2p - 1, p, 2)$. Suppose, in addition, that its support is $\{1, 2, \ldots, p\}$. Then the product $y_i z_i$, where $y_i$ and $z_i$ are respectively the $i$-th coordinates of $y$ and $z$, equals 1 or $-1$. Consider the sum $y_1 z_1 + y_2 z_2 + \cdots + y_p z_p$. Since $y \neq z$, there is at least one 1 and one $-1$ amongst the products $y_i z_i$. Since $p$ is odd and the sum is over $p$ terms, the sum is nonzero modulo $p$ and $y$ is not a solution of Eq. (2.5). Hence, $y \notin U$.

Now suppose that $\text{supp}(y) \neq \{1, 2, \ldots, p\}$. Let $J = \text{supp}(y) \cap \{1, 2, \ldots, p\}$ and $J^* = \text{supp}(y) \cap \{p + 1, p + 2, \ldots, 2p - 1\}$. Since $y$ is a solution to Eq. (2.5), $|J|$ is even. This implies $|J^*|$ is odd. Since $|J^*| < p$ and $y$ has nonzero coordinates equal to 1 or $-1$, $y$ is not a solution to Eq. (2.6). Hence, $y \notin U$. We conclude that $z$ is the only point in $B(p; 2p - 1, p, 2)$ in $U$.

To prove (c), we construct a tangent for each point $z$ in the $((\gamma - 1)p - 1)$-block $\tilde{B}(p; \gamma p - 1, p - 1)$. Permuting coordinates, it suffices to consider a point $z$ of the form

$$(a_1, a_2, \ldots, a_{tp}, 0, 0, \ldots, 0)$$

where $a_i \neq 0$ and $1 \leq i \leq \gamma - 1$. Let $W$ be the codimension-$(\gamma - 1)p - 1$ subspace defined by the system of $(\gamma - 1)p - 1$ linear equations

$$a_{j+1} x_j - a_j x_{j+1} = 0, \quad 1 \leq j \leq tp - 1, \quad (2.7)$$

and

$$x_k = 0, \quad k \in K, \quad (2.8)$$
where \( K \subseteq (tp + 1, tp + 2, \ldots, \gamma p - 1) \) and \( |K| = (\gamma - 1 - t)p \). For example, we may take \( K = (tp + 1, tp + 2, \ldots, (\gamma - 1)p) \). It is easily checked that \( z \in W \).

Let \( y \) be a point in \( B(p; \gamma p - 1, p - 1) \) and \( y = (y_1, y_2, \ldots, y_{\gamma p - 1}) \). There are several cases depending on \( \text{supp}(y) \). Suppose first that \( \{1, 2, \ldots, tp\} \not\subseteq \text{supp}(y) \). Then there is at least one index \( i \), \( 1 \leq i \leq tp \) such that exactly one of the indices \( i \) or \( i + 1 \) is in \( \text{supp}(y) \). If \( y \) is a solution of Eqs. (2.7), then the \( i \)-th linear equation implies that both \( y_i \) and \( y_{i+1} \) are zero, a contradiction. Hence \( y \not\in W \).

We may now suppose that \( \{1, 2, \ldots, tp\} \subseteq \text{supp}(y) \). If \( \text{supp}(y) = \{1, 2, \ldots, tp\} \), then Eqs. (2.7) imply that \( y \) is a nonzero multiple of \( z \), that is, \( y \) and \( z \) represent the same point in \( \text{PG}(\gamma p - 2, p) \). If \( \{1, 2, \ldots, tp\}\subseteq \text{supp}(y) \), then there are at least \( p \) indices in \( \text{supp}(y) \) and \( |\text{supp}(y) \cap K| \geq 1 \). In particular, there exists an index \( i \) in \( \text{supp}(y) \cap K \). If \( y \in W \), then Eqs. (2.8) imply that \( y_i = 0 \), a contradiction. We conclude that \( y \not\in W \). Having covered all possible cases, we conclude that \( z \) is the unique point in \( B(p; \gamma p - 1, p - 1) \) in \( W \). □

To say that \( B(p; 2p - 1, p, 1) \) is a \( 1 \)-block is equivalent to saying that in any sequence of length \( 2p - 1 \) with terms in \( \text{GF}(p) \), there is a subsequence of length \( p \) whose terms sum to zero. This was proved earlier in [3] (by elementary means) and [1] (using the Chevalley–Warning theorem). In [3], the general result, with the additive group of \( \text{GF}(p) \) replaced by a finite abelian group, was proved. (As [3] is not easily accessible, we note that the “multiplication” argument given in [1] works over an abelian group as well.) The general result, applied to the additive group of \( \text{GF}(q) \), implies that for a prime power \( q \), \( B(q; 2q - 1, q, 1) \) is a \( 1 \)-block over \( \text{GF}(q) \).

Our method can be used to obtained other kinds of blocks. We will give one example. Recall that an element \( a \) of \( \text{GF}(p) \) is a quadratic residue (respectively, nonresidue) if \( a \not= 0 \) and there exists an element \( r \) in \( \text{GF}(p) \) such that \( r^2 = a \) (respectively, if \( r^2 \not= a \) for all \( r \) in \( \text{GF}(p) \)). For \( (z_1, z_2, \ldots, z_n) \) a point in \( \text{GF}(p)^n \), let \( q_0 \) (respectively, \( q_1 \)) be the number of coordinates \( z_i \) that are quadratic residues (respectively, nonresidues). Let \( Q(p; n) \) be the set of points \( z \) in \( \text{PG}(n - 1, p) \) such that when expressed as a linear combination of the chosen basis, \( q_0 - q_1 \equiv 0 \mod p \).

**Theorem 2.2.** Let \( p \) be an odd prime and \( n > m + (p - 1)/2 \). Then \( Q(p; n) \) is an \( m \)-block.

**Proof.** We use Euler’s theorem that if \( a \not= 0 \), then \( a \) is a quadratic residue if \( a^{(p - 1)/2} = 1 \) and a quadratic nonresidue if \( a^{(p - 1)/2} = -1 \). Thus a point \( z \) is in \( Q(p; n) \) if and only if \( z \) is a solution to the polynomial equation

\[
x_1^{(p - 1)/2} + x_2^{(p - 1)/2} + \cdots + x_n^{(p - 1)/2} = 0. \tag{2.9}
\]

By the Chevalley–Warning theorem, Eqs. (2.3) and (2.9) have a common nonzero solution. The proposition now follows. □

**3. Blocks from projective algebraic varieties**

That the set \( B(p; \gamma p - 1, p - 1) \) is a \( ((\gamma - 1)p - 1) \)-block is a special case of a general theorem. A polynomial \( f(x_1, x_2, \ldots, x_0) \) with coefficients in \( \text{GF}(q) \) is homogeneous if there exists an integer \( d \) such that for all elements \( \lambda \) in \( \text{GF}(q) \), \( f(\lambda x_1, \lambda x_2, \ldots, \lambda x_0) = \lambda^d f(x_1, x_2, \ldots, x_0) \). Let \( f_j(x_1, x_2, \ldots, x_0) \), \( 1 \leq j \leq t \), be a set of homogeneous polynomials in \( n \) variables with coefficients in \( \text{GF}(q) \). The (projective algebraic) variety \( \text{Var}(f_j) \) is the set of points \( (z_1, z_2, \ldots, z_n) \) in \( \text{PG}(n - 1, q) \) such that \( f_j(z_1, z_2, \ldots, z_n) = 0 \) for all \( j \), \( 1 \leq j \leq t \).

**Theorem 3.1.** Let \( f_j, 1 \leq j \leq t \), be a set of homogeneous polynomials with \( f_j \) having total degree \( d_i \) and coefficients in \( \text{GF}(q) \). If \( n > m + \sum_{i=1}^t d_i \), then \( \text{Var}(f_j) \) in \( \text{PG}(n - 1, q) \) is an \( m \)-block over \( \text{GF}(q) \).

Theorem 3.1 gives an insight into the \( q \)-cone (also known as the \( q \)-lift) construction of Geoff Whittle [9]. Let \( B = \text{Var}(f_j) \) and \( B^* \) be the variety defined by the same polynomials \( f_j \) (but in the
variables $x_1, x_2, \ldots, x_n, x_{n+1}$ in $\text{PG}(n, q)$, the projective space of one higher dimension. Since the variable $x_{n+1}$ does not appear in any of the polynomials $f_j$, the points in $B^#$ are the points in $\text{PG}(n, q)$ of the form $(z_1, z_2, \ldots, z_n, z_{n+1})$, where $(z_1, z_2, \ldots, z_n) \in B$ and $z_{n+1} \in \text{GF}(q)$, together with the point $(0, 0, \ldots, 0, 1)$. Thus, $B^#$ is the $q$-cone of $B$ as defined in [9]. Note that $B^#$ is an $(m+1)$-block. This follows from a general result in [9] holding for all $q$-cones, or from Theorem 3.1 and the observation that since the number of variables increases from $n$ to $n+1$, $n+1 > (m+1) + \sum_{i=1}^{t} d_i$.

Acknowledgments

I thank Bruce Richter for telling me about the papers [1,3].

References