COMBINATORIAL PROBLEMS FOR ABELIAN GROUPS ARISING FROM GEOMETRY

T. SZŐNYI

Department of Computer Science,
Eötvös University, H-1088, Budapest

Received August 11, 1988

Abstract

This paper deals with elementary problems on complexes of abelian groups related to finite geometry, in particular to arcs and blocking sets of finite projective planes. Arcs contained in cubic curves led us to the notion of a 3-independent subset in abelian groups. Various examples of complete arcs containing only three points outside a conic were constructed by KORCHMÁROS [6] using $2-(m, n)$ isolated sets. In this paper we survey the known results and constructions concerning 3-independent and $2-(m, n)$ isolated sets. Moreover we obtain some new bounds for their size and give some new examples showing that the lower and upper bounds are sharp regarding their order of magnitude. Finally, we will show how the methods and constructions of the previous sections can be applied to the problem of blocking sets contained in the union of three lines and answer a question of CAMERON [1].

1. Introduction and geometric background

This paper deals with elementary problems on complexes of abelian groups arising from finite geometry. One of the central notions of finite geometry is the notion of complete arcs due to B. SEGRE (see [4], [5], [9], [10]).

A *k-arc* in a projective plane of order q is a set of k points no three of which are collinear. A k-arc is said to be *complete* if there is no $(k+1)$-arc containing it. As is well known, the maximum number of points that a k-arc can have is $q+1$ or $q+2$ according to whether q is odd or even. A k-arc with this maximum number of points is called an *oval*. Most constructions of complete arcs are based on the following general idea due to B. SEGRE, first used by LOMBARDO-RADICE [7]: 'The points of the arc, with a few exceptions, are chosen among the points of a conic, cubic (or generally: an algebraic) curve'. Taking about half the points of a conic and one point outside this conic, this construction is the "classical" SEGRE-construction. A modification of the SEGRE-construction can be found in the paper of KORCHMÁROS [6] in order to construct complete arcs containing one third or one fourth of the points of a conic and three suitably chosen extra points. His results are based on the notion of $2-(m,n)$ isolated subsets of cyclic groups. Section 2 deals with a construction of $2-(m,n)$ isolated sets in cyclic groups of order $2s$ (s even) and of order $2s+1$.

Another interesting family of complete arcs is the arcs contained in cubic curves. Several results were proved about arcs in cubic curves by DI COMITE [2], [3], SZŐNYI [12], [13], [14] and VOLOCH [15], [16]. The last two authors used the notion of '3-independent sets' introduced in [12]. Roughly speaking, the notion of a 3-independent set is the translation of 'arc' to the language of abelian groups. We also mention that the proof of the completeness of the arcs is based on the HASSE—WEIL theorem on the number of $GF(q)$-rational points of an absolutely irreducible algebraic curve defined over $GF(q)$. Lower and upper bounds for the size of a *maximal* 3-independent set can be found in Section 3.

In Section 4 we summarize the known constructions of 3-independent sets. The constructions come from [12], [13], [14], [16], but we present them in a slightly more general form. Comparing the bounds of Section 3 and the constructions of Section 4 one can say that the bounds are sharp regarding their order of magnitude.

Another important notion in finite geometry is the notion of a *blocking set.* A set B of the plane is called a blocking set if B contains no line but each line meets B. Minimal blocking sets contained in the union of three lines (i.e. blocking sets of *index three)* are related to certain complexes of abelian groups (cf. CAMERON [1]). For example using maximal 3-independent subsets we can construct various minimal blocking sets of index three. In Section 5 we answer a question of CAMERON [1], and show how the methods of Section 3 can be applied to this problem. In particular these methods yield a short proof of a theorem of SENATO [11].

2. 2-(m, n) isolated sets

First recall the definition of 2-(m,n) isolated sets and some bounds for their size due to KORCHMÁROS [6].

Definition 2.1. Given any three integers $0 < m < n < s$, a set J of integers is called 2-(m, n) *isolated* if it has the following properties:

(1) $0 \in J$,
(2) each integer in J is less than s,
(3) for every $j \in J$: $2j \not\equiv m, n \pmod{s}$; if s is even then $2j \not\equiv m, n \pmod{s/2}$,
(4) for every $j, j' \in J$: $j + j' \not\equiv m, n \pmod{s}$,
(5) if s is even, $j \not\equiv j' \pmod{s/2}$ if $j \neq j'$.

Definition 2.2. A 2-(m, n) isolated set J is called *complete with respect to (4) and (5)* if there is no $e \in J$ such that for $J \cup \{e\}$ both (4) and (5) hold.

Remark 2.1. If we consider J as a subset of the cyclic group (mod s, $+$) then (3) is equivalent to

(3′) for every $j \in J$: $4j \neq 2m, 2n$

and (5) to

(5′) for every $j \neq j' \in J$: $2j \neq 2j'$.

Therefore using (1), (3′), (4), (5′) one can define 2-(m, n) isolated sets in an arbitrary abelian group.

Define $U(s) = \{u$: there are $0 < m < n < s$ and a 2-(m, n) isolated set J complete with respect to (4) and (5) such that $|J| = u\}$.

Theorem 2.1. [6] For any $u \in U(s)$

$$s/4 \leq u \leq s/2 \text{ for } s \text{ even and } s/3 \leq u \leq s/2 \text{ for } s \text{ odd.}$$

In the above cited paper KORCHMÁROS posed the problem of constructing 2-(m, n) isolated sets which are complete with respect to (4) and (5). For small values of s he found $U(3) = \{1\}$, $U(4) = \{1, 2\}$, $U(5) = \{2\}$, $U(6) = \{2, 3\}$, $U(7) = \{3\}$.

Theorem 2.2. Let $s = 2t$, t even and $(t/2) - 1 \leq k \leq t - 1$ be fixed. Put $m = 2k + 1$, $n = 2t - 1$ and $J = \{0, 1, \ldots, k\}$. Then J is a 2-(m, n) isolated set which is complete with respect to (4) and (5).

Proof. We have to show that J is 2-(m, n) isolated and for each $a \in J$ (i.e. $k + 1 \leq a \leq 2t$) there exists a $j \in J$ such that either

$(*)$ $a + j \equiv m \pmod{s}$ or

$(**)$ $a + j \equiv n \pmod{s}$ or

$(***)$ $a \equiv j \pmod{t}$ holds.

The validity of the properties (1), (2), (4), (5) are obvious and $2j \not\equiv m, n \pmod{t}$ is a consequence of the fact that t is even since $2j \neq m, n, 2m, 2n$ regarding them as integers because the numbers m, n are odd numbers. For proving the completeness of J if $k + 1 \leq a \leq t - 1$, then $0 \leq j = t - 1 - a \leq k$ satisfies $(*)$. If $t \leq a \leq t + k$ then $0 \leq j = a - t \leq k$ satisfies $(***)$. Finally, if $t + k \leq a \leq 2t - 1$, then $0 \leq 2t - 1 - a = j \leq t - 1 - k \leq k$ satisfies $(**)$.

A similar theorem can be stated for s odd. As the proof is the same as the proof of Theorem 2.2 we omit it.

Theorem 2.3. Let $s = 2t + 1$ and $(2t + 1)/3 \leq k \leq t - 1$ be fixed. Put $m = 2k + 1$, $n = 2t$ and $J = \{0, 1, \ldots, k\}$. Then J is a 2-(m, n) isolated set which is complete with respect to (4) and (5).

This construction was used in [13] but was not stated explicitly.

Remark 2.2. Actually, our Theorems 2.2 and 2.3 show that $U(41) \supseteq \{1, \ldots 21 - 1\}$ and $U(21 + 1) \supseteq \{(21 + 1)/3, \ldots, 1\}$.

3. Bounds for the size of a maximal 3-independent subset

First we recall the definition of 3-independence.

Definition 3.1. Let G be an abelian group written additively. A subset $T \subset G$ is called *3-independent* if

$$(*) \qquad t + t' + t'' \neq 0 \text{ for every } t, t', t'' \in T.$$

A 3-independent subset $T \subset G$ is *maximal* if it is not a proper subset of an other 3-independent set.

We remark that T is 3-independent if and only if

$$(**) \quad (T + T) \cap (-T) = \emptyset, \text{ where } T + T = \{t + t' : t, t' \in T\} \text{ holds.}$$

Before obtaining bounds for the size of a maximal 3-independent subset we mention that in elementary abelian 3-groups there are no 3-independent subsets at all (as $a + a + a = 0$ for every $a \in G$ in such groups).

Theorem 3.1. Let G be an abelian group which is not an elementary abelian 3-group and $T \subset G$ be a maximal 3-independent subset. Then

$$c_1 \sqrt{|G|} \leq |T| \leq |G|/2.$$

Moreover if $|T| = |G|/2$ then there is a subgroup H of index two such that $T = G \setminus H$.

Proof. First we prove the upper bound. By $(**)$ $T + T$ and $-T$ are disjoint. Obviously $|T + T| \geq |T|$ so $|G| \geq |-T| + |T + T| \geq 2|T|$ yielding $|T| \leq |G|/2$. $|T| = |G|/2$ implies $|T| = |T + T|$ which means that T is a coset of a subgroup H. As $|T| = |H| = |G|/2$, the 3-independence of T implies $T = G \setminus H$. If $G = C_2 \times H$, $H = C_3^n$, then every 3-independent subset is contained in $G \setminus H$.

To prove the lower bound observe that the maximality of T means that for every $g \in G \setminus T$ either $g \in -(T + T)$ or $-2g \in T$ or $3g = 0$ holds. In other words $G = T \cup (-(T + T)) \cup \{g \in G : -2g \in T\} \cup \{g \in G : 3g = 0\}$. As G is not C_3^n or $C_2 \times C_3^n$, $|\{g \in G : 3g = 0\}| \leq |G|/3$. In order to estimate $|\{g \in G : -2g \in T\}|$ consider the subgroups $I = \{x \in G : 2x = 0\}$ and $D = \{y \in G : \text{there is an } x \text{ such that } y = 2x\}$. Obviously, $|D| = |G : I|$. If $-2g = t \in T$, then $t \in D \cap T$. The previously proved upper bound of this theorem, applying to $T' = T \cap D$ and D instead of T and G, yields that $|T'| \leq |D|/2$, thus $|\{g \in G : -2g \in T\}| \leq |D \cap T| \cdot |I| \leq |G|/2$. Therefore from $|G| \geq |T| + |-(T + T)| + |G|/2 + |G|/3$ it follows that $|G|/6 \leq |T| + |T|^2/2$ (as $|T + T| \leq |T| \cdot |T|/2$), hence $|T| \leq c_1 \cdot \sqrt{|G|}$. Here $c_1 = 1/\sqrt{3} - \varepsilon$.

If $|T| \neq |G|/2$ and T is a maximal 3-independent set, then the upper bound of Theorem 3.1. can be improved using the following famous theorem of KNESER (see [8, p. 6., Thm. 1.5])

Result 3.1. (the theorem of KNESER) Let A, B be two complexes of the abelian group G. Then there is a subgroup H of G such that

i) $A + B = A + B + H$

ii) $|A + B| \geq |A + H| + |B + H| - |H|$.

Theorem 3.2. Let T be a maximal 3-independent subset of the abelian group G with $|T| < |G|/2$. Then $|T| \leq 2|G|/5$. Moreover if $|T| > (|G| + 1)/3$, then there exists a subgroup $0 \neq H < G$ such that $T = T + H$ and $|T| = (|G| + |H|)/3$ where 3 is a divisor of $|G: H| + 1$.

Proof. By the theorem of KNESER there is a $H \leq G$ such that $T + T = T + T + H$ and $|T + T| \geq 2|T + H| - |H|$. By $(* *)$ $T + T \neq G$, thus $H \neq G$. Since we can suppose $|T| > (|G| + 1)/3$, $H \neq 0$ by $(* *)$ again. From $|G| \geq |T + T| + |-T| \geq 2|T + H| - |H| + |T| \geq 3|T| - |H|$ it follows that $|T| \leq (|G| + |H|)/3$. As $T + T + H = T + T$ and $(- T) \cap (T + T) = \emptyset$, $(- T + H) \cap (T + T) = \emptyset$, i.e. $T + H$ satisfies $(* *)$. The maximality of T implies that $T = T + H$. If $|H| = |G|/2$, then $|T| = |G|/2$ contrary to our assumption. The case $|H| = |G|/3$ may not occur, and similarly in case of $|H| = |G|/4$ the conditions $|T| < |G|/2$ and $T = T + H$ imply that T is a coset of H, thus $|T| \leq |G|/4$ contradicting $|T| > (|G| + 1)/3$. So if $|H| \neq |G|/2$, then $|G: H| \geq 5$. Hence $|T| \leq (|G| + |H|)/3 \leq (|G| + |G|/5)/3 = 2|G|/5$. To prove the second assertion of our Theorem 3.2 recall that $T = T + H$ and $|T + T| \geq 2|T| - |H|$. If $|T| > (|G| + 1)/3$, then in this inequality we have equality, because otherwise $|T + T| \geq 2|T|$ holds and, by $(* *)$, $|G| \geq |T + T| + |- T| \geq 2|T| + |T|$ would follow, which is a contradiction. Similarly $G \neq (T + T) \cup (- T)$ implies that $|G| \geq |T + T| + |- T| + |H| \geq 2|T| - |H| + |T| + |H| = 3|T|$, which is the same contradiction. Therefore we have $|T + T| = 2|T| - |H|$, $T = T + H$ and $G = (T + T) \cup (- T)$. Hence $|T| = (|G| + |H|)/3$ and as $|T|$ is an integer $|G: H| + 1$ is divisible by 3.

Remark 3.1. One can easily check using $T = T + H$, that from $|T| = 2|G|/5$ it follows that $T = (u + H) \cup (-u + H)$, where $u \notin H$.

Remark 3.2. The second assertion of Theorem 3.2 states that from $|T| > (|G| + 1)/3$ it follows that $|T|/|G| \in \{1/2, 2/5, \ldots, k/(3k - 1), \ldots\}$. The examples of the next section will show that these values can actually occur for $|T|/|G|$.

4. Constructions of maximal 3-independent subsets

In this section we collect the known constructions of maximal 3-independent sets. For the sake of completeness after a construction we mention its geometric consequences. Let us start with the extreme cases regarding the upper bounds mentioned in Theorems 3.1 and 3.2.

Example 4.1. Let G be even and H be a subgroup of G with $|G: H| = 2$. Then $T = G\setminus H$ is a maximal 3-independent subset of G.

Remark 4.1. The arcs corresponding to $T = G\setminus H$ were investigated by ZIRILLI [17] and VOLOCH [15] if G is the group of an elliptic cubic.

Before proving that the possible values of $|T|/|G|$ mentioned in Remark 3.2 and in Theorem 3.2 can actually occur, recall a definition and an observation from VOLOCH [16].

Definition 4.1. A 3-independent set $T \subset G$ is called *complete* if for every $y \in G\setminus T$ there are $t, t' \in T$ such that $y + t + t' = 0$. A complete 3-independent set is said to be *good* if $t \neq t'$ can be supposed in the previous condition.

(In VOLOCH's paper this was the definition of the 'maximal 3-independent set'.) Obviously, a complete 3-independent set is maximal.

Proposition 4.1. (VOLOCH) Let $f: G_1 \to G_2$ be a subjective homomorphism of finite abelian groups, and $X \subset G_2$ be a complete 3-independent set. Then $f^{-1}(X) \subset G_1$ is a complete 3-independent set.

Proof. This is Lemma 1 of VOLOCH [16].

Example 4.2. (VOLOCH) Take 1 prime $1 \equiv 2 \pmod 3$, $1 \neq 2$, $G = (\mathrm{mod}\ 1, +)$, $T = \{\pm 1, \pm 3, \ldots, \pm(2r - 1)\}$, where $r = (1 + 1)/6$. Then $|T| = 2r$ and T is a complete 3-independent subset of G.

Proof. This is §. 1. (2) of VOLOCH [16].

Proposition 4.1 shows that the groups having a subgroup of index 1 admit complete 3-independent sets with cardinality $(1 + 1)|G|/31$, i.e. the values $2/5, 4/11, \ldots, (1 + 1)/31, \ldots$ do occur for 1 prime, as $|T|/|G|$.

Example 4.3. (VOLOCH) Let 1 be a prime $1 \equiv 1 \pmod 3$, $1 \geq 13$ and $G = (\mathrm{mod}\ 1, +)$. Then $T = \{-1, 1, 3, 4, \ldots, (1 - 1)/3\}$ is a complete 3-independent set with $|T| = (1 - 1)/3$.

Proof. This is §. 1. (3) of VOLOCH [16].

Proposition 4.2. The examples of Example 4.2 are unique up to group isomorphism.

Proof. For the proof let $G = (\mathrm{mod}\ p, +)$ and T be a maximal 3-independent set of size $|T| = (p + 1)/3$. As in the theorem of KNESER (see Result 3.1) we have necessarily $H = 0$, and by §. 3. $(**)$ $|G| \geq |T + T| + |T|$ and $|T + T| \geq 2|T| - 1$, in these inequalities we have equalities if $|T| = (p + 1)/3$. (The special case of the theorem of KNESER for $(\mathrm{mod}\ p, +)$ is usually called the theorem of CAUCHY-DAVENPORT, see MANN [8, p. 3, Corollary 1.2.3]). In particular, $|T + T| = 2|T| - 1$. But in this case T is an arithmetic progression, by a theorem of VOSPER (see MANN [8, p. 3, Theorem 1.3]). So let $T = \{a_1, a_2, \ldots, a_k = a_1 + (k - 1)d\}$, $k = (p + 1)/3$. Since the map-

pings m_u: $x \to ux$ are group isomorphism, we may suppose that $d = 1$, i.e. $T = \{t_1, t_1 + 1, \ldots, t_1 + (p-2)/3\}$. T is 3-independent, hence $0 \notin T$ giving $(p+1)/3 \leq t_1 \leq p - (p-2)/3 - 1 = (2p-1)/3$. Now the only possibility for t_1 is $t_1 = (p+1)/3$, because otherwise $(2p-1)/3$ and $(2p+2)/3$ are both elements of T and this is a contradiction, because $(2p-1)/3 + (2p-1)/3 + (2p+2)/3 = 2p \equiv 0 \pmod{p}$.
Therefore $T = \{(p+1)/3, \ldots, (2p-1)/3\}$. Multiplying T by 2 we get the 3-independent sets mentioned in Example 3.2.

Using the idea of the previous proof we are able to generalize Example 3.2. This generalization shows that for every value $k/(3k-1)$ there are infinitely many groups G admitting complete 3-independent subsets of size $k|G|/(3k-1)$.

Example 4.4. Let $1 = 3k + 2$. The set $T = \{k+1, \ldots, 2k+1\}$ is a complete 3-independent subset in $(\mathrm{mod}\ 1, +)$.

Proof. We have to prove that $(T+T) \cap (-T) = \emptyset$ and $(T+T) \cup (-T) = G$. As $-(k+1) \equiv 2k+1 \pmod 1$, $T = -T$. T is an arithmetic progression, so $T+T$ is also an arithmetic progression, namely $\{2k+2, \ldots, 2(2k+1)\}$. Here $4k+2 \equiv k \pmod 1$ proving that T is a complete 3-independent set.

Now we turn to the investigation of the lower bound. The first result shows, by taking $G = (\mathrm{mod}\ p, +) \times (\mathrm{mod}\ p, +)$, that the lower bound of Theorem 3.1 is sharp regarding its order of magnitude.

Example 4.5. Let $G = A \times B$, $|A|, |B| \geq 4$ and suppose that neither A nor B is elementary abelian 3-group. Choose $a \in A$ and $b \in B$ whose order is not 3. Put

$$T = \{(a, y) : y \neq -2b\} \cup \{(x, b) : x \neq -2a\}.$$

Then T is a complete 3-independent subset in G.

Proof. As the proof of Theorem 1 of [12] can be followed step by step, we omit it.

Remark 4.2. The smallest known complete arcs of $PG(2, q)$ have cardinality $Cq^{3/4}$ and come from the complete 3-independent subsets constructed in Example 4.5 (see [12], [14], [16]).

Example 4.6. Let $G = (\mathrm{mod}\ m, +) \times (\mathrm{mod}\ n, +)$ and k be an arbitrary integer between 1 and $m/3$, where $m, n \geq 4$. The set $T = T_1' \cup T_2 \cup T_1''$ is a complete 3-independent set of G, where

$$T_1' = \{(x, y) : 1 \leq x \leq k \quad \text{and} \quad y \neq -2\},$$

$$T_2 = \{(u, 1) : u \in U = \{-2, -3, \ldots, -2k\}\},$$

$$T_1'' = \{(x, -2) : 1 \leq x \leq k \text{ and } x + u_1 + u_2 \neq 0 \text{ for every } u_1, u_2 \in U\}.$$

Moreover $k(n-1) \leq |T| \leq kn + m$.

Proof. This is a slight modification of Lemma 4 in SZŐNYI [13].

In the previous examples the direct decomposability of G played an important role. The following class of 3-independent sets shows that even in groups of prime order there are small maximal 3-independent subsets.

Example 4.7. Let $1/2 \leq \alpha < 1$ be fixed. Choose a prime q between $p^\alpha/2$ and $p^\alpha/4$ and let m_1 be the maximal integer which is relatively prime to q and satisfies $m_1 q < p/2$. Now $m_1 + 2q > p/2$. Suppose that $p \equiv k \pmod m$, $m = m_1 q$ and let $k \equiv a_1 q + a_2 m_1 \pmod m$. (Here a_1, a_2 are uniquely determined.) Put

$A_1 = \{cq\colon 0 \leq c < m_1 \text{ but } c \neq a_1, 2a_1\} \cup \{dm_1\colon 0 \leq d < q \text{ but } d \neq a_2, 2a_2\}$

and finally let $A = A_1 \cup \{a_1 + m\colon a_1 \in A_1\}$.

Then A is a 3-independent subset of $G = (\text{mod } p, +)$. Moreover $|A| \leq 2(q + m_1) \leq 10p^\alpha$, and $|G \setminus (A + A)| \leq 10q + 6m_1 \leq 20p^\alpha$. Therefore a maximal 3-independent set B containing A satisfies $|B| \leq 20p^\alpha$.

Proof. This is Theorem 2.1. of [14].

Finally, we summarize the information contained in sections 3 and 4 in a theorem.

Theorem 4.1. Let G be an abelian group which is not an elementary abelian 3-group, and $T \subset G$ be a maximal 3-independent subset. Then

a) $c_1 \sqrt{|G|} \leq |T| \leq |G|/2$,

b) if $|T| \geq (|G| + 1)/3$, then $|T| = (|G| + |H|)/3$ where $|G\colon H| \equiv 2 \pmod 3$ and for every $1 \equiv 2 \pmod 3$ there are infinitely many groups G having a complete 3-independent subset of size $(1 + 1)|G|/31$.

c) for every $0 < c \leq 1/3$ and $\varepsilon > 0$, there is a maximal 3-independent set T of $G = (\text{mod } p, +) \times (\text{mod } p, +)$ satisfying $(c - \varepsilon)|G| \leq |T| \leq (c + \varepsilon)|G|$.

d) for every fixed α, $1/2 \leq \alpha < 1$ there are C_1, C_2 such that for every $p > p_0$ prime $(\text{mod } p, +)$ has a maximal 3-independent subset T satisfying

$$C_1 p^\alpha \leq |T| \leq C_2 p^\alpha.$$

5. Blocking sets of index three: a translation for abelian groups

Definition 5.1. A subset S of a finite projective plane is called a *blocking set* if S meets every line but contains no line. A blocking set S is *minimal* if $S \setminus \{x\}$ is not a blocking set for every $x \in S$. The following definition due to CAMERON [1] is related to certain blocking sets. This connection will be explained in Proposition 5.3.

Definition 5.2. Let G be an additive abelian group of order n, and m a positivei nteger. We say that $G \to m$ if there are nonempty subsets A, B, C of G such that

(i) $0 \notin A + B + C$;
(ii) (A, B, C) is maximal subject to (i);
(iii) $|A| + |B| + |C| = m$.

Proposition 5.1.

a) If $|G| = n$ and $G \to m$ then $3(\sqrt{n + 1/4} - 1/2) \leq m \leq 3n/2$,

b) If Θ: $G \to H$ in an epimorphism and $H \to m$, then $G \to \frac{|G|m}{|H|}$.

c) $G \to n + d$ for any proper divisor d;of n.

Proof. This is §. 3. (3.4.) in CAMERON [1, p. 49].

We remark that the upper and the lower bounds are essentially sharp.

Example 5.1. Let $G = (\text{mod } p, +) \times (\text{mod } p, +)$, $A = \{(x, x^2)$: $x = 0, 1, \ldots, p - 1\}$, $B = \{(-x, -x^2)$: $x = 0, 1, \ldots, p - 1\}$, and $C = \{(0, y)$: $y = 1, 2, \ldots, p - 1\}$. Then (A, B, C) shows that $G \to 3p - 1$.

Proof. One can easily check that $A + B = G \setminus C$, $A + C = G \setminus A = G \setminus (-B)$, $B + C = G \setminus B = G \setminus (-A)$ proving $G \to 3p - 1$.

As a partial converse to Proposition 5.1. (c) we prove the following.

Proposition 5.2. If $G \to m$ with $m > |G| + 1$, then there is a subgroup H of G such that $m = |G| + |H|$.

Proof. The proof of Theorem 3.2 based on the theorem of KNESER proves Proposition 5.2 as well, so we give only the outlines of the proof. Let $A, B, C \subset G$ show that $G \to m$. Choose a subgroup H to A, B by the theorem of KNESER (Result 3.1). Here obviously $H \neq G$ and by $m > |G| + 1$ we get $H = 0$. Now $A + B = A + B + H$ and $|A + B| \geq |A + H| + |B + H| - |H|$. By the maximality of (A, B, C) necessarily $A = A + H$, $B = B + H$, $C = C + H = G \setminus (A + B)$. Again $m > |G| + 1$ implies that $|A + B| = |A + H| + |B + H| - |H|$ thus $|A| + |B| + |C| = |G| + |H|$.

As a by-product we obtained a theorem of SENATO [11]; if $m = 3|G|/2$, then A, B, C are cosets of a subgroup of index two.

As complete 3-independent sets yield triplets (A, A, A) showing $G \to 3|A|$, the results contained in Theorem 4.1 can be applied in the present case. Finally, mention should be made of the geometric consequences of the results.

Definition 5.3. A blocking set S is called ablocking set of *index three* if it is contained in the union of three lines.

Theorem 5.1. Let S be a minimal blocking set of index three. Then one of the following holds:

i) $|S| = 2q$
ii) $|S| = 3(q - 1)$
iii) $|S| = 3q + 1 - m$, where $(GF(q), +) \to m$, and $q > 2$
iv) $|S| = 3q - m$, where $GF(q)^* \to m$.

Proof. This is §. 3. (3. 5.) in CAMERON [1].

6. References

1. CAMERON, P. J.: Four lectures on Projective Geometries, In: Finite Geom. (ed.: Baker, C. A. and Batten, L. M.) Lecture Notes in pure and applied math. *103*, Marcel Dekker (1985), 27—63.
2. DI COMITE, C.: Su k-archi deducibili da cubiche piane, Atti Accad. Naz. Lincei Rend. *33*, (1962), 429—435.
3. DI COMITE, C.: Intorno a certi $(q + 9)/2$-archi completi, Atti Accad. Naz. Lincei Rend. *36* (1964), 819—824.
4. HIRSCHFELD, J. W. P.: Projective Geometries over Finite Fields, Oxford Univ. Press, 1979.
5. KÁRTESZI, F.: Introduction to Finite Geometries, Akadémiai Kiadó, Budapest, 1976.
6. KORCHMÁROS, G.: New Examples of k-arcs in PG(2, q), Eur. J. Comb. *4* (1983), 329—334.
7. LOMBARDO-RADICE, L.: Sul problema dei k-archi completi di $S_{2,g}$ Boll. Un. Mat. Ital. *11* (1956), 178—181.
8. MANN, H. B.: Addition theorems, John Wiley, 1965.
9. SEGRE, B.: Lectures on Modern Geometry, Cremonese, Roma, 1961.
10. SEGRE, B.: Introduction to Galois Geometries, (ed.: Hirschfeld, J. W. P.) Atti Accad. Naz. Lincei Memorie *8* (1967).
11. SENATO, D.: Blocking sets di indice tre, Rend. Accad. Sci. Fis. Mat. Napoli *49* (1982), 89—95.
12. SZŐNYI, T.: Small complete arcs in Galois planes, Geom. Ded. *18* (1985), 161—172.
13. SZŐNYI, T.: Note on the order of magnitude of k for complete k-arcs in $PG(2, q)$, Discrete Math. *66* (1987), 279—282.
14. SZŐNYI, T.: Arcs in cubic curves and 3-independent subsets in abelian groups, Colloq. Math. Soc. J. Bolyai *52* (1988), 499-508
15. VOLOCH, J. F.: On the completeness of certain plane arcs, Eur. J. Comb. *8* (1987), 453—456.
16. VOLOCH, J. F.: On the completeness of certain plane arcs II, Eur. J. Comb., *11* (1990), 491-496
17. ZIRILLI, F.: Su una classe di k-archi di un piano di Galois, Atti Accad. Naz. Lincei Rend. *54* (1973), 393—397.

Tamás SZŐNYI Department of Computer Science, Eötvös University, H-1088, Budapest, Múzeum krt. 6—8. HUNGARY