CWI Quarterly Volume 9 (1 & 2) 1996, pp. 31 – 35

# Special Point Sets in Finite Projective Planes

Aart Blokhuis
*Technical University Eindhoven, Department of Mathematics,*
*P.O. Box 513, 5600 MB Eindhoven The Netherlands*
*e-mail* aartb@win.tue.nl

We consider the following three problems:

1. Let $U$ be a $q$-subset of $GF(q^2)$ with the properties $0, 1 \in U$ and $u - v$ is a square for all $u, v \in U$. Does it follow that $U$ consists of the elements of the subfield $GF(q)$? Here $q$ is odd.

2. Let $f : GF(q) \to GF(q)$ be any function, and let

$$D_f = \left\{ \frac{f(x) - f(y)}{x - y} \; : \; x \neq y, \, x, y \in GF(q) \right\}$$

   be the set of difference quotients (directions, slopes). What are the possibilities for $|D_f|$?

3. Let $B$ be a subset of $PG(2, q)$, the Desarguesian projective plane of order $q$, such that every line contains at least one point of $B$. What are the possibilities for $|B|$?

The third problem is the oldest of the three. The subset $B$ is called a *blocking set*. To make the problem interesting we restrict ourselves to *minimal* blocking sets, that is blocking sets not containing a proper subset that is still a blocking set. The smallest possible blocking set is always a line. The most interesting problem is the next possible size. Essentially the problem is due to RICHARDSON [15] who considered the plane of order 3, although already in [11] it is mentioned that the only minimal blocking sets in the Fano plane $PG(2, 2)$ are the lines. In $PG(2, 3)$ the next possible size is 6. The problem was made popular by DI PAOLA [12] who determined the next possible size in the planes of order 4, 5, 7, 8 and 9 (answers: 7, 9, 12, 13 and 13). The most general result for the size of a blocking set in arbitrary (not necessarily Desarguesian) projective planes is BRUEN's result [8]

*A minimal blocking set $B$ in a projective plane of order $n$ is either a line, or contains at least $n+\sqrt{n}+1$ points with equality if and only if $B$ consists of the points of a Baer subplane.*

The second problem is mentioned in [14] as one of the applications of Rédei's theory of lacunary polynomials. Rédei's result is that unless the points are all on a line, either the number of difference quotiens is large: at least $(q+1)/2$, or the number is in an interval of the form

$$\left[1+\frac{q-1}{p^e+1},\ \frac{q-1}{p^e-1}\right],$$

for some $e = 1, \ldots, \lfloor n/2 \rfloor$, where $q = p^n$. In the particular case that $q = p$ is prime these intervals are not there, and the lower bound was improved to $(p+3)/2$ by Megyesi, a student of Rédei. One of RÉDEI's challenges in his book [14] was to find a more direct proof of this result. For this special case (that $q$ is an odd prime) such a proof was given by LOVÁSZ and SCHRIJVER [10] together with a characterization of the corresponding function. It turns out that essentially $f(x) = x^{(q+1)/2}$.

The connection between problems 2 and 3 comes from the observation that a blocking set can be formed by starting with the graph of a function $f : GF(q) \to GF(q)$ in the affine plane $AG(2,q)$, and then adding on the line at infinity the points corresponding to slopes determined by this graph. In this way a blocking set of size $q + |D_f|$ is obtained. Although these blocking sets seem to be very special, in fact all known examples of 'small' blocking sets are of this form (we say that a blocking set is *small* if its size is less than $q + (q+3)/2$).

The first problem finally comes from a conjecture by van Lint and MACWILLIAMS [13] and has to do with the characterization of the vectors of minimum weight in quadratic residue codes. It can be related to problem 2 as follows: If we identify the field $GF(q^2)$ with the affine plane $AG(2,q)$ in a suitable way (respecting the vector space structure over $GF(q)$, then the set $U$ turns in to a set of points, and the condition that $u - v$ is always a square means that the collection of directions determined by $U$ is contained in the set of $(q+1)/2$ 'square' directions. If $q$ is prime, this shows then that $U$ is a line (and since $0, 1 \in U$ in fact $GF(q)$) by the result of Megyesi/Lovász-Schrijver.

The first problem was completely settled in the positive in [1]. The basic idea was to consider the polynomial (in $GF(q^2)[X]$)

$$f(X) = \prod_{u \in U} (X - u).$$

One has to show that under the conditions in the problem $f(X) = X^q - X$. In other words, most of the elementery symmetric functions of the set $U$ have to vanish. This was accomplished by a number of tricks and geometric considerations that somehow worked, but precisely why remains obscure.

As a consequence of these investigations we became very interested in problems 2 and 3. To get a feeling for problem 2 consider the following examples of

functions determining few directions. Again $q = p^n$ and $q_1 = p^e$ where $e \mid n$ so that $GF(q_1)$ is a subfield of $GF(q)$.

Example 1. $f(x) = x^{q_1}$. In this case $(f(x) - f(y))/(x - y) = (x - y)^{q_1 - 1}$, and the number of $(q_1 - 1)$-th powers is exactly $(q - 1)/(q_1 - 1)$. This shows that the upper bound in the Rédei intervals can be realized for those intervals where $e \mid n$.

Example 2. $f(x) = \mathrm{Tr}_{q \to q_1}(x) = x + x^{q_1} + x^{q_1^2} + \ldots + x^{q/q_1}$. In this case

$$\frac{f(x) - f(y)}{x - y} = \frac{\mathrm{Tr}(x - y)}{x - y},$$

and it is an exercise to show that $\mathrm{Tr}(z)/z$ takes on exactly $q/q_1 + 1$ different values. This shows that the lower bound in Rédei's interval is approximately correct, again for $e \mid n$.

There are other examples but they give a number of directions between the above two limits. In fact the description of the known examples with at most $(q + 1)/2$ directions is best given in a more geometric way: The affine plane $AG(2, q)$, or better the vector space $GF(q)^2$ can also be considered as a vector space of dimension $2d$ over a subfield $GF(q_1)$ of $GF(q)$, where $q = q_1^d$. If $U$ is a $d$-dimensional subspace of this vector space, then $U$ has $q$ points, and it will determine a number of directions in the interval $[q/q_1 + 1, (q - 1)/(q_1 - 1)]$ (assuming that $q_1$ was choosen maximal for $U$). A set $U$ like this will be called $GF(q_1)$-linear. The above examples where first described in the more general setting of translation planes in [7].

Our most recent result almost completely settles the second problem [6]:

*Let $U \subset GF(q)^2$ be a point set of size $q$ containing the origin, let $D$ be the set of slopes of secants of $X$, and put $N := |D|$. Let $e$ (with $0 \le e \le n$) be the largest integer such that each line with slope in $D$ meets $U$ in a multiple of $p^e$ points. Then we have one of the following:*

(i) *$e = 0$ and $(q + 3)/2 \le N \le q + 1$,*

(ii) *$e = 1$, $p = 2$, and $(q + 5)/3 \le N \le q - 1$,*

(iii) *$p^e > 2$, $e \mid n$, and $q/p^e + 1 \le N \le (q - 1)/(p^e - 1)$,*

(iv) *$e = n$ and $N = 1$.*

*Moreover, if $p^e > 3$ or ($p^e = 3$ and $N = q/3 + 1$), then $U$ is $GF(p^e)$-linear, and all possibilities for $N$ can be determined explicitly (in principle).*

The line of attack on this problem is basically due to Rédei, although the approach in [5] is perhaps more transparant. Associated to the set $U$ in the affine plane $AG(2, q)$ is now a polynomial in two variables (the Rédei polynomial)

$$r(X, Y) = \prod_{(u_1, u_2) \in U} (X + u_1 Y - u_2) = \sum_{j=0}^{q} \rho_j(Y) X^j.$$

For $y \in GF(q)$, let $r_y(X) := r(X, y)$. Then $r_y$ is a monic polynomial of degree $q$ in $X$. This polynomial codes the intersection sizes of the lines in direction $y$ with $U$ - indeed, these intersection sizes are the multiplicities of the roots of $r_y$. If $y$ is not a secant direction, then we see all possible roots with multiplicity one:

$$r_y(X) = X^q - X \Leftrightarrow y \notin D.$$

It follows that $\rho_j = 0$ if $1 < j < q$ and $j \geq N$; indeed, we have found $q - N$ distinct zeros of the polynomial $\rho_j(Y)$ which has degree at most $q - j$ (in fact one more with the correct definition of $\rho_j(\infty)$).

If $y$ is a secant direction, then $r_y$ becomes a polynomial that factors in linears, and has a lot of vanishing coefficients. It is here that the technical part starts, which consists of the investigation of such polynomials. This finally leads to the conclusion that $\rho_j = 0$ unless $j$ is a power of $p^e$, and the result follows.

Finally we consider the third problem. Using Rédei's results, but not his techniques the lower bound for blocking sets in Desarguesian planes of non-square order was first improved to $q + \sqrt{2q} + 1$ [3, 9], but it was clear that in order to get a substantial improvement not just his results, but the theory behind it should somehow be made to work.

That this was possible was finally demonstrated in [2], where for the case $q = p$ the lower bound was proved to be indeed $p + (p + 3)/2$. This lead to new inspiration for the problem of characterizing small blocking sets and work by Szőnyi [16] gives a major step in this direction. His main result gives Rédei-type intervals for the size of small blocking sets:

*Let $B$ be a small minimal blocking set in $PG(2, q)$, $q = p^n$. Then*

$$q + 1 + \frac{q}{p^e + 2} \leq |B| \leq \frac{qp^e + 1 - \sqrt{(qp^e + 1)^2 - 4q^2p^e}}{2},$$

*for some integer $e$, $1 \leq e$. The order of magnitude of the upper bound is $q + 2q/p^e$.*

Again the principal idea is to investigate the associated Rédei polynomial but now with the aid of results from Algebraic Geometry on the structure of curves with many rational points.

This is still work in progress. The obvious first step to be taken now is that the intervals in Szőnyi's theorem should be restricted to those coming from subfields, that is $e \mid n$. Much more should be true however:

Conjecture: *Small minimal blocking sets are of Rédei type.*

References


1. A. Blokhuis (1984). On subsets of $GF(q^2)$ with square differences, *Indag. Math.*, **46**, 369–372.
2. A. Blokhuis (1994). On the size of a blocking set in $PG(2, p)$, *Combinatorica* **14**, 11–114.

3. A. Blokhuis and A.E. Brouwer (1986). Blocking Sets in Desarguesian Projective Planes, *Bull. London Math. Soc.*, **18**, 132–134.
4. A. Blokhuis (1996). *Blocking sets in Desarguesian Planes*, in: Paul Erdős is Eighty, vol. **2**, 1–23. ed.: D. Miklós, V.T. Sós, T. Szőnyi, Bolyai Soc. Math. Studies.
5. A. Blokhuis, A.E. Brouwer & T. Szönyi (1995). The number of directions determined by a function $f$ on a finite field, *J. Comb. Th. (A)* **70**, 349-353.
6. A. Blokhuis, S. Ball, A.E. Brouwer, L. Storme and T. Szőnyi . On the number of slopes of the graph of a function defined on a finite field. *Manuscript.*
7. A.E. Brouwer and H.A. Wilbrink (1982). Blocking sets in translation planes, *J. of Geometry*, **19**, 200.
8. A.A. Bruen (1971). Blocking sets in finite projective planes, *SIAM J. Appl. Math.*, **21**, 380–392.
9. A.A. Bruen and R. Silverman (1987). Arcs and Blocking Sets II, *Europ. J. Combinatorics*, **8**, 351–356.
10. L. Lovász and A. Schrijver (1981). Remarks on a theorem of Rédei, *Studia Scientiarum Mathematicarum Hungarica*, **16**, 449–454.
11. J. von Neumann and O. Morgenstern (1947). *Theory of Games and Economic Behavior*, 2nd ed., Princeton Univ. Press, Princeton.
12. J. di Paola (1966). On a restricted class of block design games, *Canad. J. Math.*, **18**, 225–236.
13. J.H. van Lint and F.J. MacWilliams (1978). Generalized Quadratic Residue Codes, *IEEE Transactions on Information Theory,* IT **24**, 730–737.
14. L. Rédei (1970). *Lückenhafte Polynome über endlichen Körpern,* Birkhäuser Verlag, Basel.
15. M. Richardson (1956). On finite projective games, *Proc. Amer. Math. Soc.*, **7**, 458–465.
16. T. Szőnyi. Blocking Sets in Desarguesian Affine and Projective Planes, *Manuscript.*