Studia Scientiarum Mathematicarum Hungarica 16 (1981), 449—454

REMARKS ON A THEOREM OF RÉDEI

L. LOVÁSZ and A. SCHRIJVER

Dedicated to the memory of László Rédei

In his monograph [1], Rédei developed a theory which led to a characterization of certain fully reducible lacunary polynomials over finite fields. His book concludes with a selection of very interesting and highly non-trivial applications of the theory to various problems in algebra and number theory, such as the Hajós theory of abelian groups, divisibility maximum properties of gaussian sums etc. He raises the problem whether a more direct proof of any of these applications can be given. In this note we give a rather simple proof of one of these applications, and show that some of the others can be obtained from this. We also give two new applications, one motivated by design theory and the other one concerning automorphism groups of graphs. Some other results obtained by Rédei as applications of his theory seem to need the full strength of the theory.

1. A theorem on affine planes

The following result is essentially equivalent to Theorem 24′ in [1].

THEOREM 1. *Let p be a prime and let X be a subset of the affine plane $AG(2, p)$, such that $|X|=p$ and X is not a line. Then X determines at least $(p+3)/2$ directions.*

Here we say that a direction is *determined by* X if X contains two points spanning a line in this direction.

Clearly, if $|X|>p$ then X determines all the $p+1$ directions, since in this case at least one line from every parallel class contains more than one point of X.

PROOF. We may assume that X does not determine all directions. Then $AG(2, p)$ can be coordinatized in such a way that

$$X = \{(k, b_k)\colon k\in GF(p)\} \tag{1}$$

where $b_0, \dots, b_{p-1}\in GF(p)$. Let U be the collection of directions determined by X, where each direction is identified by its "slope", i.e.

$$U = \left\{\frac{b_k-b_m}{k-m}\colon k, m\in GF(p),\ k \neq m\right\}. \tag{2}$$

1980 *Mathematics Subject Classification.* Primary 51E15; Secondary 12C05.

Key words and phrases. Lacunary polynomials, finite fields, directions determined by point sets, Hajós theory, Paley graphs.

To derive a contradiction suppose that $|U|<\frac{p+3}{2}$. Consider the polynomials

$$F_j(x) = \sum_{k\in GF(p)} (b_k-kx)^j \tag{3}$$

for $j=0, \ldots, p-2$. Since

$$\sum_{k\in GF(p)} k^j = 0 \quad \text{iff} \quad j=0 \quad \text{or} \quad p-1\nmid j, \tag{4}$$

we have $\deg F_j\leqq j-1$ for $j\neq 0$.

If $x\notin U$, then the elements b_k-kx $(k\in GF(p))$ are all distinct. Hence by (4), $F_j(x)=0$ if $x\notin U$. Since $\deg F_j\leqq j-1$, it follows that F_j is the zero polynomial if $j-1<p-|U|$, in particular if $j\leqq(p-1)/2$.

Using that every function over $GF(p)$ is a polynomial of degree at most $p-1$, we may write

$$b_k = c_m k^m+\ldots+c_2k^2+c_1k+c_0, \tag{5}$$

where $c_m\neq 0$, $m\leqq p-1$. Since X is not a line, we have $m\geqq 2$. Let

$$p-1 = am+b, \tag{6}$$

where $a>0$ and $0\leqq b\leqq m-1$. As $m\geqq 2$, it follows easily that $a+b\leqq(p-1)/2$. So $F_{a+b}=0$, in particular the coefficient of x^b is 0 in F_{a+b}. This coefficient is

$$0 = \sum_k \binom{a+b}{b} b_k^a k^b = \binom{a+b}{b} \sum_k \left(c_m^a k^{am+b}+\sum_{j=b}^{p-2} d_j k^j\right) \tag{7}$$

with some field elements d_j, by (5). Using (4) we get for this same coefficient

$$\binom{a+b}{b} c_m^a \sum_k k^{p-1} = -\binom{a+b}{b} c_m^a \neq 0. \tag{8}$$

This is a contradiction.

Supplement. *If a p-element subset X of $AG(2, p)$ determines exactly $(p+3)/2$ directions, then in a suitable coordinate system it can be written in the form*

$$X = \{(k, k^{\frac{p+1}{2}}): k\in GF(p)\}. \tag{9}$$

(Hence, X is contained in the lines $x=y$ and $x=-y$.)

Proof. Applying linear transformations if necessary, we may assume that in (5) we have $c_m=1$ and $c_{m-1}=c_1=c_0=0$.

If a and b defined by (6) satisfy $a+b<(p-1)/2$ then we get a contradiction in the same way as before. So suppose that $a+b=(p-1)/2$. It is easy to see that this is possible only if either $m=2$ or $m=(p+1)/2$. In the first case we have the set $X=\{(k, k^2): k\in GF(p)\}$, which determines p directions. So we must have $m=(p+1)/2$. It suffices to show that in (5) all coefficients but the first vanish. Suppose indirectly that this is not the case, and let c_{m-t} be the first non-vanishing coefficient after the leading term. By the assumptions made above, we have $2\leqq t\leqq$

$\leqq m-2$. Consider the coefficient of x^{t-2} in F_t. This must vanish, since $t \leqq m-2 = (p-3)/2$. But this coefficient is

$$(10) \qquad \sum_k \binom{t}{2} b_k^2 k^{t-2} = \binom{t}{2} \sum_k \left(k^{p+1} + 2c_{m-t} k^{p+1-t} + \sum_{j=1}^{p+1-t-1} d_j k^j\right) k^{t-2}$$

with some field-elements d_j. Using (4) we get

$$(11) \qquad -\binom{t}{2} 2c_{m-t} \neq 0,$$

a contradiction.

2. Applications

2.1. Rédei's formulation of Theorem 1 is the following:

If $f: GF(p) \to GF(p)$ is non-linear then the difference quotient

$$(12) \qquad \frac{f(x)-f(y)}{x-y} \quad (x, y \in GF(p);\ x \neq y)$$

assumes at least $(p+3)/2$ distinct values.

This clearly follows from Theorem 1 by considering the "graph" of f.

2.2. Another one of Rédei's applications of his theory, specialized here for the case of prime fields, is the following.

Let $f: GF(p) \times GF(p) \to GF(p)$ be a mapping such that (i) f is linear in its first variable, and (ii) the number of values of the first variable for which f is one-to-one in the second variable is at least $(p+1)/2$. Then $f(x, y) = g_1(x)h(y) + g_2(x)$, where g_1 and g_2 are linear and h is one-to-one.

This can be obtained from Theorem 1 as follows. Write, by (i),

$$(13) \qquad f(x, y) = a(y)x + b(y),$$

and let

$$X = \{(a(y),\ b(y)): y \in GF(p)\}.$$

We claim that X determines at most $(p+1)/2$ directions. In fact, if a "non-vertical" direction with slope t is determined by X, then

$$(14) \qquad \frac{b(y)-b(z)}{a(y)-a(z)} = t$$

and hence

$$(15) \qquad a(y)t - b(y) = a(z)t - b(z),$$

and thus $f(-t, y)$ is not a one-to-one function of y. So by (ii), there are at most $(p-1)/2$ non-vertical slopes determined by X. With the possible vertical slope, there are at most $(p+1)/2$ directions determined by X. Hence by Theorem 1, X must be a line, i.e. $(a(y), b(y)) = h(y)(a, b) + (c, d)$ for some $(a, b) \neq (0, 0)$, (c, d), and some one-to-one mapping h. Setting $g_1(x) = ax + b$ and $g_2(x) = cx + d$, the result follows.

Applying the Supplement to Theorem 1, the same argument proves that if instead of (ii) we assume that the number of values of the first variable for which f is one-to-one in the second variable is exactly $(p-1)/2$, then

$$f(x,y) = g_1(x)h(y)^{\frac{p+1}{2}} + g_2(x)h(y) + g_3(x) \tag{16}$$

where g_1, g_2, g_3 are linear and h is one-to-one. This statement is essentially the same as Theorem 22 in Rédei's book.

2.3. Let G be an additively written abelian group and $A, B \subseteq G$. We write

$$G = A+B \tag{17}$$

if every element of G can be written uniquely as $a+b$, $a \in A$, $b \in B$. Motivated by Hajós' theorem, Rédei proved the following:

If $G \cong Z_p \oplus Z_p$ then in every decomposition (17) *such that* $0 \in A, B$, *one of A and B is a subgroup.*

It is quite natural to try to deduce this result from Theorem 1, since G is naturally isomorphic with $AG(2,p)$. From $G=A+B$ it easily follows that apart from trivial cases, $|A|=|B|=p$. Furthermore, no direction is determined by both A and B. For, consider e.g. the "horizontal" direction and let $\xi(g)$ denote the first coordinate of $g \in G$. Let, further, ε be a primitive p^{th} root of unity. Then

$$\Big(\sum_{a\in A} \varepsilon^{\xi(a)}\Big)\Big(\sum_{b\in B} \varepsilon^{\xi(b)}\Big) = p\sum_{j=0}^{p-1} \varepsilon^j = 0,$$

and so one of the factors on the left, say the first, is 0. But then $\xi(a)$ $(a \in A)$ ranges through all residue classes $\bmod p$, i.e. the horizontal direction is not determined by A.

Thus one of A and B determines at most half of all directions, i.e. at most $(p+1)/2$ directions. By Theorem 1, this subset is a line, i.e. in G it is a coset of a subgroup. Since it contains 0, it is a subgroup.

Further on, Rédei proves the following result:

Let $G \cong Z_p \oplus Z_p$ and let $A \subseteq G$, $|A|=p$. Assume that A is not a subgroup. Then there are at most $(p-1)/2$ subsets B containing 0 for which (17) holds.

By the preceding, every such subset B must be a subgroup of order p. But then B corresponds in $AG(2,p)$ to a line through the origin. (17) easily implies that every line parallel to B must intersect A, and hence the direction of B is not determined by A. By Theorem 1, there are at most $(p-1)/2$ such directions.

3. Two more applications

3.1. J. H. Van Lint has the following conjecture. If q is a prime power and $X \subseteq GF(q^2)$ such that $|X|=q$, $0, 1 \in X$ and the difference of any two elements in X is the square of an element of $GF(q^2)$, then $X=GF(q)$. This conjecture was proved for $q=p$ a prime by Van Lint and F. J. MacWilliams (unpublished). We show here that it follows also from Theorem 1. (The case of general q remains open.)

In fact, $GF(p^2)$ may be considered as an affine plane over $GF(p)$. Since every element of $GF(p)$ is a square, for $x, y \in GF(p^2)$ the fact whether or not $x-y$ is a square depends only on the direction of the line of this affine plane connecting x and y. It is easy to see that there are $(p+1)/2$ directions which correspond to squares this way and $(p+1)/2$ directions which do not. Hence X determines at most $(p+1)/2$ directions and thus by Theorem 1, it is a line. Since $0,1 \in X$, it follows that $X = GF(p)$.

3.2. The *Paley graph* of order p (p is a prime of the form $4k+1$) is the graph whose vertices are the elements of $GF(p)$, two of them being adjacent iff their difference is a square in $GF(p)$. It is clear that if $a, b \in GF(p)$, then

$$x \mapsto a^2x+b \tag{18}$$

is an automorphism of the Paley graph. It follows from the work of Carlitz [2] and McConnel [3] (see also [4]) that the Paley graph has no other automorphisms. This can be derived also from Theorem 1 (or, rather, from the result in 2.1) rather easily. For let

$$f\colon\ GF(p) \mapsto GF(p) \tag{19}$$

be an automorphism of the Paley graph. Then if $x-y$ is a square then $f(x)-f(y)$ is a square and if $x-y$ is a non-square then $f(x)-f(y)$ is a non-square. Thus it follows that

$$\frac{f(x)-f(y)}{x-y} \tag{20}$$

is always a square. So the difference quotient (20) takes at most $(p-1)/2$ values (it is never 0 since f is one-to-one). By 2.1, this implies that

$$f(x) = cx+b$$

for some $b, c \in GF(p)$. Since (20) must be a square, c must be a square, i.e. $c=a^2$ for some $a \in GF(p)$.

4. Concluding remarks

4.1. The main difficulty in Rédei's results is in the case when the underlying finite field is not a prime field. Whether or not the proof method of this paper can be extended to this case is not clear. The formulation of the results is certainly more complex.

Example. Let

$$X = GF(p)\times GF(p) \subsetneqq GF(p^2)\times GF(p^2) = AG(2, p^2). \tag{21}$$

Then the slope of any line determined by X is either ∞ or an element of $GF(p)$. Thus X determines only $p+1$ directions.

For the formulation of the corresponding generalization of Theorem 1 we refer to Rédei's book (Theorem 24).

4.2. But even for the case of prime fields Rédei's theory yields more than Theorem 1. One of his results is the following

THEOREM. *Let* $a_1, \ldots, a_p \in GF(p)$ *be such that* $\sum_{i=1}^{p} a_i^j = 0$ *for* $j = 1, \ldots, \frac{p-1}{2}$. *Then either all the* a_i *are equal or all of them are distinct.*

In spite of the striking similarity with the proof of Theorem 1, we could not deduce this result from Theorem 1.

REFERENCES

[1] RÉDEI, L., *Lacunary polynomials over finite fields,* North-Holland Publishing Co., Amsterdam—London; American Elsevier Publishing Co., Inc., New York, 1973. *MR* **50** # 4548.

[2] CARLITZ, L., A theorem on permutations in a finite field, *Proc. Amer. Math. Soc.* **11** (1960), 456—459. *MR* **22** # 8005; **22**—2547.

[3] MCCONNEL, R., Pseudo-ordered polynomials over a finite field, *Acta Arith.* **8** (1962/63), 127—151. *MR* **29** # 2244.

[4] BRUEN, A. A. and LEVINGER, B. W., A theorem on permutations of a finite field, *Canad. J. Math.* **25** (1973), 1060—1065. *MR* **48** # 8452.

(Received January 29, 1982)

JÓZSEF ATTILA TUDOMÁNYEGYETEM
BOLYAI INTÉZETE
ARADI VÉRTANÚK TERE 1
H—6720 SZEGED
HUNGARY

MATHEMATISCH CENTRUM
2E BOERHAAVESTRAAT 49
AMSTERDAM
THE NETHERLANDS