MATH. SCAND. 74 (1994), 5–8

AN ADDITION THEOREM IN A FINITE ABELIAN GROUP

JØRGEN CHERLY

1. Introduction.

We say that a subset A of a finite abelian group G is an additive basis if there exists an integer h such that any element of G can be written as a sum of at most h elements of A. The set A is said to be an additive basis of order h in case h is minimal. We denote by $|A|$ the cardinality of the set A.

Let F_q be a finite field of $q = p^m$, $m \in \mathsf{N}$ elements and let $\mathsf{F}_q[X]$ denote its polynomialring. The degree of a polynomial $a \in \mathsf{F}_q[X]$ is denoted $\delta^0 a$.

A subset A of $\mathsf{F}_q[X]$ is said to be an additive basis if there exists an integer h such that any element of $\mathsf{F}_q[X]$ can be written as a sum of at most h elements of A. The set A is said to be an additive basis of order h in case h is minimal.

The Snirel'man density dA of A is given by

$$dA = \inf_{n \geqq 0} q^{-n-1} \operatorname{card} A_n,$$

where $A_n = \{a \in A \mid \delta^0 a \leqq n\}$, see [1] [2] [3].

For any integer n, let $G_n = \{f \in \mathsf{F}_q[X] \mid \delta^\circ f \leqq n\}$. It is clear that $(G_n, +)$ is a finite abelian group of order $|G_n| = q^{n+1}$.

We prove here the following results:

THEOREM 1.1. *Let A be a subset of G which contains 0. If A is an additive basis of order h for G then*

$$h \leqq 2[|G|/|A|]$$

This inequality is optimal.

Theorem 1.1 implies the following addition theorem in $\mathsf{F}_q[X]$.

THEOREM 1.2. *Let A be a subset of* $\mathsf{F}_q[X]$ *such that*

(i) $0 \in A$

(ii) $dA > 0$

(iii) *For any* $n \geqq 0$: A_n *is an additive basis for* G_n

Received June 9, 1992.

Then A is an additive basis of order at most 2 $[1/dA]$.

In [1] we obtained the estimate $h \leqq 1/(dA)^2$. J. M. Deshouillers proved in [3] that A is an additive basis of order at most $4/dA$. Our proof is different and we improve the constant factor from 4 to 2.

2. Preliminary results.

Let $(G, +)$ be a finite abelian group. We shall denote by $A, B, C, \ldots$ non empty subsets of G. We define the addition of sets of group elements by $A + B = \{a + b \mid a \in A, b \in B\}$. We shall need the following two theorems from H. B. Mann's book [4] chapter 1.

THEOREM 2.1. *Either* $A + B = G$ *or* $|G| \geqq |A| + |B|$

THEOREM 2.2. *If* $C = A + B$ *then* $|C| \geqq |A| + |B| - |H|$ *where H is the subgroup*

$$H = \{g \in G \mid C + g = C\}$$

3. Some lemmas.

LEMMA 3.1. *Let* $C = A + B$, *where A and B are non empty subsets of G, and* $0 \in B$. *Then either* $C + B = C$ *or* $|C| \geqq |A| + |H|$ *where H is the subgroup* .

$$H = \{g \in G \mid C + g = C\}$$

PROOF. Assume $C + B \neq C$, then $C + B \supset C$ since $0 \in B$. Hence we can find elements $b_0 \in B$ and $c_0 + b_0 \notin C$. Since $C + b_0$ is a union of complete cosets of H we have

$$C + b_0 = \bigcup_{c \in C} \{c + b_0 + H\} = \bigcup_{a \in A} \{a + b_0 + H\} \bigcup_{c \in C \setminus A} \{c + b_0 + H\}$$

Now for any $a \in A$ we have

$$\{a + b_0 + H\} \cap \{c_0 + b_0 + H\} = \varnothing$$

Indeed let $a_0 \in A$ be such that $a_0 + b_0 + h_1 = c_0 + b_0 + h_2$ with $h_1, h_2 \in H$. Then $c_0 + b_0 \in a_0 + b_0 + H \subseteq C$, contrary to the fact that $c_0 + b_0 \notin C$.

It follows that

$$C + b_0 \supset \{A + b_0\} \cup \{c_0 + b_0 + H\}$$

Hence

$$|C| = |C + b_0| \geqq |A + b_0| + |c_0 + b_0 + H| = |A| + |H|$$

LEMMA 3.2. *Let $C = A + B$, where A and B are non empty subsets of G, and $0 \in B$. Then either*
$C + B = C$ or

$$|C| \geqq |A| + \frac{1}{2}|B|$$

PROOF. (for the non abelian case see J. E. Olson [5]). Assume that $C + B \supset C$. Hence by Theorem 2.2 and lemma 3.1

$$2|C| \geqq 2|A| + |B|$$

LEMMA 3.3. *Let A be a non empty subset of $G, 0 \in A$ and $k \geqq 2$: Then either $kA = (k+1)A$ or $|kA| \geqq \frac{k+1}{2}|A|$.*

PROOF. (see also J. E. Olson [6] Theorem 2.2). Assume $kA \neq (k+1)A$. Then $mA \neq (m+1)A$ for all m such that $2 \leqq m \leqq k$.
By lemma 3.2 with $A \to (m-1)A$, $B \to A$ we obtain

$$|mA| \geqq |(m-1)A| + \frac{1}{2}|A| \text{ for all } m \text{ such that } 2 \leqq m \leqq k$$

Hence $\sum_{m=2}^{k} |mA| \geqq \sum_{m=2}^{k} |(m-1)A| + \frac{k-1}{2}|A|$
which implies $|kA| \geqq \frac{k+1}{2}|A|$

4. Proof of Theorem 1.1.

Define the integer k_0 by $k_0 = [|G|/|A|]$. Assume $k_0 A \neq G$. Then by lemma 3.3 and the definition of k_0

$$|k_0 A| \geqq \frac{k_0+1}{2}|A| > \frac{|G|}{2}.$$

Whence by theorem 2.1 we have $2k_0 A = G$.

The inequality in Theorem 1.1 is optimal. Indeed let A be any subset of G such that $|A| = [(|G|+2)/2]$. Then by Theorem 2.1, A is an additive basis of order 2. Also $2k_0 = 2[|G|/|A|] = 2$ for $|G| \neq 2$.

5. Proof of Theorem 1.2.

By (i), (ii), (iii) and Theorem 1.1 we have: For any $n \geqq 0$: A_n is a basis of order h_n for G_n with

$$h_n \leqq 2\,[q^{n+1}/|A_n|] \leqq 2\,[1/dA]$$

It is then clear that any element of $\mathsf{F}_q[X]$ can be written as a sum of at most $2\,[1/dA]$ elements of A.

REFERENCES

1. J. Cherly, *Addition theorems in* $\mathsf{F}_q[X]$, J. Reine Angew. Math. 293/294 (1977), 223–227.
2. J. Cherly, *On complementary sets of group elements*, Arch. Math. (Basel) 35 (1980), 113–118.
3. J. Cherly and J. M. Deshouillers, *Un théorème d'addition dans* $\mathsf{F}_q[X]$, J. Number Theory 34 (1990).
4. H. B. Mann, *Addition Theorems*, New-York, London, Sydney 1965.
5. John E. Olson, *On the Sum of Two Sets in a Group*, J. Number Theory 18 (1984), 110–120.
6. John E. Olson, *Sums of sets of group elements*, Acta Arith. 28 (1975), 147–156.

UNIVERSITE DE BRETAGNE OCCIDENTALE
6, AVENUE LE GORGEU
29287 BREST CEDEX
FRANCE