Europ. J. Combinatorics (1991) **12**, 211–221

On the Subsets Product in Finite Groups

YAHYA OULD HAMIDOUNE

Let B be a proper subset of a finite group G such that either $B = B^{-1}$ or G is abelian. We prove that there exists a subgroup H generated by an element of B with the following property. For every subset A of G such that $A \cap H \neq \emptyset$, either $H \subset A \cup AB$ or $|A \cup AB| \geq |A| + |B|$. This result generalizes the Cauchy–Davenport Theorem and two theorems of Chowla and Shepherdson.

1. INTRODUCTION

The following result was proved independently by Cauchy [4] and Davenport [6].

THEOREM 1.A (The Cauchy–Davenport Theorem). *Let p be a prime number, and let A and B be two proper subsets of $\mathbb{Z}_p$. Then $|A + B| \geq \min(|A| + |B| - 1, p)$.*

Using the Davenport transfer argument, Chowla and Shepherdson proved the following two results.

THEOREM 1.B (Chowla [5]). *Let A and B be two proper subsets of $\mathbb{Z}_n$ such that B contains 0 and all the elements of $B\backslash\{0\}$ are units of $\mathbb{Z}_n$. Then either $A + B = \mathbb{Z}_n$ or $|A + B| \geq |A| + |B| - 1$.*

THEOREM 1.C (Shepherdson [15]). *Let A and B be two proper subsets of a finite abelian group G such that $B \subset A$. Then either $|A \cup (A + B)| \geq |A| + |B|$ or there is $b \in B$ such that $A \cup (A + B)$ contains the subgroup generated by b.*

As a consequence of Theorem 1.C, Shepherdson obtained the following:

THEOREM 1.D (Shepherdson [15]). *Let G be a finite abelian group and let S be a subset of G. Let $k \in \mathbb{N}$ be such that $k|S| \geq |G|$. Then there is a sequence of natural numbers $(n_s; s \in S)$ such that $\sum n_s s = 0$ and $1 \leq \sum n_s \leq k$.*

The last result is only stated by Shepherdson for $\mathbb{Z}_n$ and $\mathbb{Z}_n^*$, but his method works for all finite abelian groups.

In [9] we proved the following:

THEOREM 1.E ([9]). *Let G be a finite group and let S be a non-empty subset of G. Then there is a non-void sequence of elements of S with product equal to 1 and length at most $\lceil |G|/|S| \rceil$.*

We did not realize in [9] that our result was a generalization of Shepherdson's Theorem 1.D to the non-abelian case. Indeed, we have only just become aware of Shepherdson's result.

In [9] we obtained a more general lower bound for the length of a cycle in a graph with a transitive group of automorphisms.

0195-6698/91/030211 + 11 $02.00/0

Recently, Theorem 1.D was rediscovered by Alon [1]. His approach uses a result of Scherk [14]. Alon used Theorem 1.D to prove the following:

THEOREM 1.F (Alon [1]). *For every $\varepsilon > 0$ and $k > 1$, there is some natural number n_0 such that for every $n > n_0$, and every subset $A \subset \mathbb{Z}_n$ satisfying*

$$|A| > \left(\frac{1}{k} + \varepsilon\right)n,$$

there is a subset of A with zero sum and cardinality at most k.

In a note added in proof, Alon pointed out that Theorem 1.F is also valid for any abelian group of odd order [1].

Our main result is the following.

Let S be a subset of a finite group G such that $S = S^{-1}$ or G is abelian. We show that there exists a subgroup H generated by an element of S with the following property. For every subset A of G such that $A \cap H \neq \emptyset$, either $H \subset A \cup AS$ or $|A \cup AS| \geqslant |A| + |S|$.

This result generalizes the Cauchy–Davenport Theorem 1.A, Chowla's Theorem 1.B and Shepherdson's Theorem 1.C. As a consequence we obtain the following generalization of Alon's Theorem 1.F.

For every $\varepsilon > 0$ and $k > 1$, there is some natural number n_0 such that, for every $n > n_0$, and every subset $A \subset \mathbb{Z}_n$ satisfying

$$|A| > \left(\frac{1}{k} + \varepsilon\right)n,$$

there is a non-zero element of A all of the multiples of which can be expressed as a sum of a subset of A of cardinality at most k.

Our proofs are based on some properties of the atoms in Cayley graphs established in [7–11]. We recall some definitions and results in Section 2. We also give some proofs for the convenience of the reader.

2. PRELIMINARIES

The smallest integer $\geqslant r$ will be denoted by $\lceil r \rceil$. The cardinality of a set V will be denoted by $|V|$. The diagonal of $V \times V$ will be denoted by $\Delta(V)$. By a *graph* we mean a graph of an anti-reflexive relation. Such a graph may be defined as an ordered pair (V, E), where V is a set and E is a subset of $V \times V \backslash \Delta(V)$. Let X be a graph. The vertex-set of X will be denoted by $V(X)$. Similarly, the edge-set of X will be denoted by $E(X)$. Let A be a subset of $V(X)$ and let $E[A] = \{(x, y) \in E(X) \mid x, y \in A\}$. The subgraph $X[A]$ of X *induced* by A is the graph $(A, E[A])$. The graph X is said to be *complete* if $E(X) = V(X) \times V(X) \backslash \Delta(V(X))$.

Let X be a graph and let A be a subset of $V(X)$. The set of vertices incident from A will be denoted by $\Gamma_X^+(A)$, or simple $\Gamma^+(A)$. More precisely, $\Gamma_X^+(A) = \{y \in V(X): \exists x \in A$ such that $(x, y) \in E(X)\}$. We denote $\Gamma_X^+(A) \backslash A$ by $N_X^+(A)$. Letting $x \in V(X)$, we write $\Gamma^+(x) = \Gamma^+(\{x\})$ and $d_X^+(x) = |\Gamma_X^+(x)|$. We recall that $d_X^+(x)$ is called the *outdegree* of x. If all the vertices have the same outdegree, the graph is said to be *outregular*. Let X be an outregular graph. The outdegree of any vertex of X will be called the outdegree of X and will be denoted by $d^+(X)$.

Let $X = (V, E)$ be a graph. The *inverse* graph of X is the graph $X^{-1} = (V, E^{-1})$, where $E^{-1} = \{(x, y) \mid (y, x) \in E\}$. Let A be a subset of $V(X)$ and let x be a vertex. We

put $\Gamma^+_{X^{-1}}(A) = \Gamma^-_X(A)$. Similarly, we define $N^-_X(A)$ and $d^-_X(x)$. We call $d^-_X(x)$ the *indegree* of x with respect to X. The graph X is said to be *inregular* if X^{-1} is outregular.

A sequence of distinct vertices $[x_1, x_2, \ldots, x_k]$ such that (x_i, x_{i+1}) is an edge, $1 \leqslant i \leqslant k-1$, is said to be a *path* from x_1 to x_k with length $k-1$. Of course, we admit the case $k = 1$, where the path consists of a single vertex.

Let $X = (V, E)$ be a graph containing two vertices x and y. A set of paths from x to y is said to be *openly* disjoint if the intersection of any pair of these paths is equal to $\{x, y\}$. The maximum number of openly disjoint paths connecting x to y will be denoted by $\tau(x, y)$. We put $\tau(X) = \min(\tau(x, y): x \neq y \text{ and } x, y \in V(X))$.

Now assume that (x, y) is not an edge. A set of the form $N^+(A)$, where $x \in A$ and $y \notin (A \cup N^+(A))$ is said to *separate* y from x. The minimum cardinality of a set separating y from x will be denoted by $\kappa(x, y)$. It is obvious that $\tau(x, y) \leqslant \kappa(x, y)$.

THEOREM 2.A (Menger). *Let x and y be two vertices of a graph X such that (x, y) is not an edge of X. Then $\kappa(x, y) = \tau(x, y)$.*

This result is well known and several proofs exist. A short proof may be found in [12].

THEOREM 2.B (Menger). *Let X be a graph. Let A and B be two subsets of $V(X)$ such that $|A| = |B| = \tau(X)$. Then there are $\tau(X)$ disjoint paths from A to B.*

PROOF. In order to deduce Theorem 2.B from Theorem 2.A, we add two vertices u and v and add the edge-set $\{(u, x) \mid x \in A\} \cup \{(y, v) \mid y \in B\}$. Now $\kappa(u, v) \geqslant \tau(X)$. By Theorem 2.A, there are $\tau(X)$ openly disjoint paths from u to v. □

A graph X is said to be *strongly connected* if for all $x, y \in V(X)$ there is a path connecting x to y. Note that a graph with one vertex is strongly connected. Let X be a graph. A subset C of $V(X)$ such that $X[C]$ is strongly connected and which is maximal with respect to this property is called a *component* of X. Note that X is strongly connected if X^{-1} is strongly connected. A proper subset A of $V(X)$ is said to be a *source* if $N^-_X(A) = \varnothing$. A *sink* of X may be defined as a source of X^{-1}.

The following lemma is well known and easy.

LEMMA 2.C. *If not strongly connected, a finite graph contains at least two components, of which one is a source and another is a sink.*

In the last part we shall use a Ramsey argument due to Alon. We summarize this method below.

Let G be a finite group containing a subset S and an element x. A non-void sequence of elements of S with product equal to x will be called a *factorization* of x with respect to S.

Let G be a finite abelian group. Take $r(G)$ to be the maximal cardinality of a subset A of G such that $x + y \neq 2z$, for any $x, y, z \in A$ with $x \neq y$.

THEOREM 2.D (a corollary of Roth's theorem [13]). *For any $\varepsilon > 0$ there exists some natural number n_0 with the following property. If $n > n_0$ then $r(\mathbb{Z}_n) \leqslant \varepsilon n$.*

THEOREM 2.E (Brown and Buhler [3]). *For any $\varepsilon > 0$ there exists n_0 with the following property. For every abelian group of odd order at least n_0, $r(G) \leqslant \varepsilon n$.*

THEOREM 2.F (Alon [1]). *Let A be a subset of an Abelian group G satisfying $|A| \geqslant n/k + (1+\sqrt{3(k-2)})r(G) + 1$. Then there is a subset B of $A\backslash\{0\}$ of order at most n/k such that the sum of any factorization of length no more than k with respect to B may also be expressed as the sum of a non-void subset of A of cardinality at most k.*

PROOF. The proof is just an adaptation of Alon's proof for proposition 2.5 of [1]. □

3. ATOMS

Let us give some definitions.

Let X be a non-complete strongly connected graph and let F be a subset of $V(X)$. We say that F is a *positive prefragment* of X if $F \neq \emptyset$ and $F \cup N^+(F) \neq V(X)$. If so, we put $\bar{F} = V(X)\backslash(F \cup N^+(F))$. A positive prefragment of X^{-1} is said to be a *negative* prefragment of X. A *separating set* of X is a set of the form $N^+(F)$, where F is a positive prefragment of X.

REMARK. Every non-complete strongly connected graph has a positive prefragment. Any non-void subset of a positive prefragment is also a positive prefragment of X.

Let X be a strongly connected graph. The *connectivity* $\kappa(X)$ of X is defined as follows:

$$\kappa(X) = \min\{|N^+(F)| \mid F \text{ is a positive prefragment of } X \text{ or } |F| = 1\}.$$

It follows that the connectivity of a non-complete graph is the minimal cardinality of a separating set.

LEMMA 3.1. *Let X be a strongly connected graph. Then $\kappa(X) = \kappa(X^{-1})$. If X is non-complete then $\kappa(X) = \tau(X) = \min(\kappa(x, y)\colon (x, y) \notin E(X))$.*

LEMMA 3.2 [7]. *Let X be a non-complete strongly connected graph and let A be a non-void subset of $V(X)$. Then $|N^+(A)| \geqslant \min(\kappa(X), |V(X) - A|)$.*

We say that F is a *positive fragment* of X if F is a positive prefragment of X and if $|N_X^+(F)| = \kappa(X)$. A positive fragment of X^{-1} is said to be a *negative fragment* of X.

Let $a_+(X)$ be the minimal cardinality of a positive fragment of X. Let $a(X) = \min(a_+(X), a_+(X^{-1}))$.

A positive (respectively, negative) fragment of X with cardinality $a(X)$ is said to be a *positive* (respectively, *negative*) *atom* of X. Note that the atoms of a graph might all be positive or all be negative.

LEMMA 3.3([7], Section 2). *Let X be a non-complete strongly connected graph and let F be a positive fragment of X. Then $\bar{F}$ is a negative fragment of X.*

Therefore $(F, N^+(F), \bar{F})$ is a partition of $V(X)$ into a positive fragment, a minimum separating set and a negative fragment. It follows that the cardinality of an atom is less than $|V(X)|/2$.

LEMMA 3.4 ([7], Section 2). *Let X be a non-complete strongly connected graph and let A be a positive atom of X. Then $X[A]$ is strongly connected.*

The definitions immediately imply the following:

LEMMA 3.5 [7]. *Let X be a non-complete strongly connected graph. Then $\kappa(X) \leqslant \min(d^+(x);\ x \in V(X))$. Moreover, the equality holds if X has a positive atom of cardinality* 1.

The following result is the basic property of atoms:

PROPOSITION 3.6 ([7], Proposition 1). *Let X be a non-complete strongly connected graph. Let A be a positive atom of X and let F be a positive fragment of X having a non-void intersection with A. Then A is contained in F.*
In particular, two distinct positive atoms are disjoint.

We shall use the following easy lemma:

LEMMA 3.7. *Let X be a strongly connected graph and let A be a subset of $V(X)$. Then $\kappa(X[V\backslash A]) \geqslant \kappa(X) - |A|$.*

More details about these questions may be found in [7–9].

4. CAYLEY GRAPHS

A graph X is said to be *vertex-transitive* if its group of automorphisms acts transitively on its vertex-set. It is an easy exercise to show that a (finite) vertex-transitive graph X is outregular and inregular. Moreover, $d^+(X) = d^-(X)$. An important class of vertex-transitive graphs is the class of Cayley graphs defined below.

Let G be a group and let S be a subset of $G\backslash\{1\}$. The *Cayley graph* of G with respect to S is the graph $\mathrm{Cay}(G, S) = (G, E)$, where $E = \{(x, y) \mid x^{-1}y \in S\}$. The *subgroup generated* by S will be denoted by $\langle S\rangle$. Letting $a \in G$, the left translation $x \to ax$ will be denoted by γ_a.

REMARK. Let $X = \mathrm{Cay}(G, S)$. If F is a subset of G, then $N_X^+(F) = (FS)\backslash F$.

REMARK. Let G be a finite group and let S be a subset of $G\backslash\{1\}$. A factorization of an element $x \in G\backslash\{1\}$ with respect to S determines a unique path with the same length from 1 to x and vice versa.

LEMMA 4.1. *Let G be group and let S be a subset of $G\backslash\{1\}$. For every element of G, γ_a is an automorphism of* $\mathrm{Cay}(G, S)$. □

REMARK. If $\mathrm{Cay}(G, S)$ has a positive atom, then there is a unique positive atom of $\mathrm{Cay}(G, S)$ containing 1. Indeed, let B be any positive atom of $\mathrm{Cay}(G, S)$ and let $a \in B^{-1}$. By Lemma 4.1, aB is a positive atom. The uniqueness follows by Proposition 3.6.

LEMMA 4.2. *Let G be a finite group and let S be a subset of $G\backslash\{1\}$. Then any connected component of* $\mathrm{Cay}(G, S)$ *induces a graph isomorphic to* $\mathrm{Cay}(\langle S\rangle, S))$. *In particular,* $\mathrm{Cay}(G, S)$ *is strongly connected iff S is a generating set.*

PROPOSITION 4.3 ([9], Theorem 3.1). *Let G be a finite group and let S be a subset of $G\backslash\{1\}$. Let A be a positive atom of* Cay(G, S) *containing* 1. *Then A is a subgroup generated by $S \cap A$. The other positive atoms are exactly the left cosets modulo A.*

PROOF. Let $x \in A$. By Lemma 4.1, xA is a positive atom. But $xA \cap A \neq \emptyset$. By Proposition 3.6, $xA = A$. Therefore A is closed under product. Hence A is a subgroup (observe that A is finite).

Let $x \in A$. By Lemma 3.4, there is a path $[x_0, x_1, \ldots, x_{k-1}, x_k]$ contained in $X[A]$ such that $x_0 = 1$ and $x_k = x$. Let $s_i = x_i^{-1}x_{i+1}$, for $0 \leq i \leq k-1$. By the definition of Cay(G, S), we have $s_i \in S$, for $0 \leq i \leq k-1$. Since A is a subgroup, we have $s_i \in A$, for $0 \leq i \leq k-1$. It follows that $x = \Pi s_i \in \langle S \cap A \rangle$.

By Lemma 4.1 any left coset modulo A is a positive atom. Now any positive atom intersects one of the left cosets, and coincides with it by Proposition 3.6. □

We need the following results.

PROPOSITION 4.4 ([11], Corollaire 2.2). *Let G be a finite abelian group and let S be a subset of $G\backslash\{0\}$. Let A be a positive atom of* Cay(G, S). *Then A is also a negative atom of X.*

PROOF. We may assume that $0 \in A$, by Lemma 4.1.

By Proposition 4.3, A is a subgroup. It is easily verified that the mapping $x \to -x$ is an a isomorphism from Cay(G, S) onto Cay$(G, -S)$. It follows that $-A = A$ is a positive atom of Cay$(G, -S) = (\text{Cay}(G, S))^{-1}$. Hence A is a negative atom of Cay(G, S). □

COROLLARY 4.5 ([11], Corollaire 2.3). *Let A be an atom of an abelian Cayley graph. Then $N^+(A)$ is a union of cosets modulo A. In particular, $|A|$ divides $\kappa(X)$.*

REMARK. Let X be an abelian Cayley graph. By the above results, there is a unique atom containing 0 which is both positive and negative.

5. Well Connected Subsets

Let $X = (V, E)$ be a graph and let A be a subset of V. We say that A is *well connected* if $\tau(x, y) = d^+(x)$ for all $x, y \in A$ such that $x \neq y$.

LEMMA 5.1. *Let G be a finite group, let S be a subset of $G\backslash\{1\}$ and let A be a well connected subset of* Cay(G, S) *containing* 1. *Then for every $x \in A$ there is a non-void factorization of x with length at most $\lceil |G|/|S| \rceil$.*

PROOF. Let $x \in A$. Take $n = |G|$ and $s = |S|$.

Case 1: $x \neq 1$. Since A is well connected there are s openly disjoint paths (μ_i) from 1 to x. We clearly have $2 + \sum(|\mu_i| - 2) \leq n$. It follows that there is some i such that $|\mu_i| \leq (n + 2s - 1)/s$. It follows that $|\mu_i| \leq \lceil n/s \rceil + 1$. This path corresponds to a factorization of x with respect to S with length $\leq \lceil n/s \rceil$ (cf. Remark 2, Section 4).

Case 2: $x = 1$. The factorization exists by Theorem 1.E. □

Let $X = (V, E)$ be a graph and let A and B be subsets of V such that $|A| = |B| = k$. A set of k disjoint paths from A to B containing only vertices of $A \cup B \cup C$ is called a

k-linking from A onto B over C.

PROPOSITION 5.2. *Let $X = (V, E)$ be a graph and let A be a positive fragment of X. Let B be a subset of $N^+(A)$ and let C be a subset of $B \cup (V\backslash(A \cup N^+(A)))$. If B and C are of the same cardinality, then there is a linking from B onto C over $V\backslash(A \cup N^+(A))$.*

PROOF. Let $X' = X\backslash(N^+(A)\backslash B)$. By Lemma 3.7, $\kappa(X') \geq \kappa(X) - |N^+(A)\backslash B| = |B|$. By Menger's Theorem 2.B, there are $|B|$ disjoint paths from B to C in X'. Since $N^+_{X'}(A)$ is a subset of B these paths cannot intersect A. Observe that a path which intersects A must use an element of $N^+_{X'}(A) \subset B$ distinct from its origin. This contradicts the assumption that the paths are simple and disjoint. Also, the vertices of these paths are contained in $(V\backslash(N^+(A)) \cup B$. Hence this linking from B to C is over $V\backslash(A \cup N^+(A))$. □

COROLLARY 5.3. *Let $X = (V, E)$ be a graph and let A be a negative fragment of X. Let B be a subset of $N^-(A)$ and let C be a subset of $B \cup (V\backslash(A \cup N^-(A)))$ be such that $|C| = |B|$. Then there is a linking from C onto B over $V\backslash(A \cup N^-(A))$ such that $|B| = |C|$.*

PROOF. The proof follows by applying Proposition 5.2 to X^{-1}. □

THEOREM 5.4. *Let G be a finite group and let S be a nonvoid subset of $G\backslash\{1\}$ such that $S = S^{-1}$. Then there exists $s \in S$ such that the subgroup generated by s is well connected in* Cay(G, S).

THEOREM 5.5. *Let G be a finite abelian group and let S be a non-void subset of $G\backslash\{1\}$. Then there exists $s \in S$ such that the subgroup generated by s is well connected in* Cay(G, S).

We give a common proof for these two theorems below.

PROOF OF THEOREMS 5.4 AND 5.5. Suppose the theorem false and take a counter-example with minimal order. We prove the following points.

I. $\langle S \rangle = G$. Since Cay(G, S) is a counter-example, Cay$(\langle S \rangle, S)$ is also a counter-example. By the minimality of $|G|$, we have $G = \langle S \rangle$. It follows that $X =$ Cay(G, S) is strongly connected. We see easily that X is a non-complete graph, since otherwise G is well connected. Let A be an atom of X containing 1.

II. $\kappa(X) < |S|$ *and* $S \cap A \neq \emptyset$. We have $\kappa(X) < |S|$, since otherwise G is well connected by Menger's Theorem 2.A. By Lemma 3.5, we have $|A| > 1$. By Proposition 4.3, A is a subgroup generated by $S \cap A$. In particular, $S \cap A \neq \emptyset$.

III. The atom A is both positive and negative. This is obvious if $S = S^{-1}$, since $N^+(A) = N^-(A)$. It follows from Proposition 4.4, when G is abelian. Let $Y =$ Cay$(A, S \cap A)$. If $S = S^{-1}$ (respectively, G is abelian), we have $S \cap A = S^{-1} \cap A^{-1} = (S \cap A)^{-1}$ (respectively, A is abelian). By the minimality of $|G|$, there is some $s \in S \cap A$ such that $H = \langle s \rangle$ is well connected in Y. By our hypothesis, there are two elements x and y of H such that $\tau_X(x, y) < |S|$.

Put $B = N^+(x)\backslash A$, $C = N^-(y)\backslash A$, $T = N^+(A)$, $K = T\backslash N^+(x)$ and $K_0 = K \cap N^-(y)$.

IV. We have $B \subset T$ *and* $C \subset N^-(A)$. These relations follows obviously from the definitions.

V. $|C| = |B| = |S \backslash A|$ *and* $|K| < |S \cap A| < |A|$. We clearly have $|S| = |N^+(x)| = |N^+(x) \cap A| + |N^+(x) \backslash A| = |S \cap A| + |B|$. Similarly, $|S| = |N^-(x)| = |N^-(x) \cap A| + |N^-(x) \backslash A| = |S \cap A| + |C|$. It follows that

$$|K| = |T - N^+(x)| = |T - B| = |T| - |B| < |S| - |B| = |S \backslash B|.$$

Therefore, we have $|K| < |S \backslash B| = |S \cap A| < |A|$.

VI. $\tau_Y(x, y) = |S \cap A|$. This follows since $\langle s \rangle$ is well connected in Y.

VII. There is a subset $U_0 \subset G \backslash (A \cup N^-(A) \cup K)$ *and a linking from* U_0 *onto* K_0 *over* K. The set $F = G \backslash (A \cup N^-(A))$ is a fragment. By *V*, We have $|K| = |K_0| + |K \backslash K_0| < |A| \leq |F|$. We see easily that $K_0 \subset N^+(A) \cap N^-(A)$ and hence $K_0 \cap F = \emptyset$. It follows that $|K_0| \leq |K - F| \leq |F - K|$. Let U be a subset of $F \backslash K$ such that $|U| = |K_0|$.

By Corollary 5.3 and III, there is a linking from U onto K_0 over $G \backslash (A \cup N^-(A))$. The origins of this linking belong to $G \backslash K$, while the ends belong to K_0. We define U_0 to be the set of last elements of this linking not belonging to K. It is clear that U_0 satisfy the required property.

VIII. There is a linking from B *onto* C *over* $G \backslash A$. We clearly have $|U_0| = |K_0|$. Let $W = (C \backslash K) \cup U_0$. Since $U_0 \cap N^-(A) = \emptyset$ and $C \subset N^-(A)$, we have $C \cap U_0 = \emptyset$. Using *V*, we have

$$|W| = |U_0| + |C \backslash K| = |K_0| + |C \backslash K_0| = |C| = |B|.$$

Also, $W \cap (A \cup T) = (U_0 \cap (T \backslash K)) \cup ((C \backslash K) \cap T) \subset T \backslash K = B$.

By Proposition 5.2, there is a linking from B onto W over $G \backslash (A \cup K)$. We form a linking from B onto C by composing this linking with the linking from U_0 onto K_0 found in VII.

By VI, there are $|S \cap A|$ openly disjoint paths from x to y contained in A. Using VII, we form $|B|$ openly disjoint paths from x to y by composing x, the linking from B to C and y. It is clear that the resulting $|B| + |S \cap A|$ paths are openly disjoint.

It follows using *V* that $\tau(x, y) \geq |B| + |S \cap A| = |S \backslash B| + |B| = |S|$.

This relation contradicts the last part of III.

This contradiction proves the theorem. □

6. The Subsets Product

THEOREM 6.1. *Let* B *be a subset of a finite group* G *such that* $B = B^{-1}$. *There exists an element* b *of* B *with the following property. For every subset* A *of* G *such that* $A \cap \langle b \rangle \neq \emptyset$, *either* $|A \cup (AB)| \geq |A| + |B|$ *or* $\langle b \rangle \subset A \cup (AB)$.

PROOF. The result is obvious if $1 \in B$. Suppose the contrary.

Take $X = \mathrm{Cay}(G, B)$. By Theorem 5.4, there exists $b \in B$ such that $\langle b \rangle$ is well connected. Take $H = \langle b \rangle$ and suppose $H \backslash (A \cup (AB)) \neq \emptyset$. Let $x \in A \cap H$ and let $y \in H \backslash (A \cup (AB)) = H \backslash (A \cup N^+(A))$. It follows that $N^+(A)$ separates y from x. Therefore

$$|N^+(A)| \geq \kappa(x, y) \geq \tau(x, y). \tag{1}$$

By Theorem 5.4, we have $\tau(x, y) = |B|$. Using (1), we have $|N^+(A)| \geq |B|$. Therefore $|A \cup (AB)| = |A \cup N^+(A)| = |A| + |N^+(A)| \geq |A| + |B|$. □

THEOREM 6.2. *Let B be a subset of a finite abelian group G. There exists an element b of B with the following property. For every subset A of G such that $A \cap \langle b \rangle \neq \emptyset$, either $|A \cup (A+B)| \geq |A| + |B|$ or $\langle b \rangle \subset A \cup (A+B)$.*

PROOF. The proof is the same as for Theorem 6.1, except that it uses Theorem 5.5 instead of Theorem 5.4. □

COROLLARY 6.3 (Chowla's Theorem 1.B). *Let A and B be two subsets of $\mathbb{Z}_n$ such that B contains 0 and all the elements of $B\backslash\{0\}$ are units of $\mathbb{Z}_n$. Then either $A+B=\mathbb{Z}_n$ or $|A+B| \geq |A| + |B| - 1$.*

PROOF. Take $B' = B\backslash\{0\}$. Assume that $|A+B| < |A| + |B| - 1$. Therefore $|A \cup (A+B')| < |A| + |B'|$. By Theorem 6.2, there is an element b of B' such that $\langle b \rangle$ is contained in $A \cup (A+B') = A+B$. Since b is a unit, we have $A+B=\mathbb{Z}_n$. □

REMARK. We included the above proof only to show that Theorem 6.2 is a generalization of Theorem 1.B and hence for the Cauchy–Davenport Theorem.

A quick proof for the Cauchy–Davenport Theorem based on the atoms uses only the relation $\kappa(\mathrm{Cay}(\mathbb{Z}_p, B')) = |B'|$ (cf. Corollaire 2 of [7]). We note that Chowla's Theorem can be obtained easily from Proposition 4.3.

COROLLARY 6.4 (Shepherdson's Theorem 1.C). *Let G be a finite abelian group and let A, B be two proper subsets of G such that $B \subset A$. Then either $|A \cup (A+B)| \geq |A| + |B|$ or there is $b \in B$ such that $\langle b \rangle \subset A \cup (A+B)$.*

PROOF. The result is obvious if $0 \in B$. Suppose the contrary.

By Theorem 6.2, there exists $b \in B$ with the following property. For all subsets C of G with $C \cap \langle b \rangle \neq \emptyset$, either $|C \cup (C+B)| \geq |C| + |B|$ or $\langle b \rangle \subset C \cup (C+B)$. But $b \in B \subset A$. Hence either $\langle b \rangle \subset A \cup (A+B)$ or $|A \cup (A+B)| \geq |A| + |B|$. □

COROLLARY 6.5. *Let A, B be two non-empty subsets of a finite abelian group G such that B is a subset of A. Then either $|A \cup (A-B)| \geq |A| + |B|$ or there is $b \in B$ such that $\langle b \rangle \subset A \cup (A-B)$.*

The proof is similar to the proof of Corollary 6.4.

Corollary 6.5 is the dual of Shepherdson Theorem 1.C. We note also that the method used by Shepherdson works for Corollary 6.5.

We show below that Theorem 1.C is valid in the non-abelian case in which $B = B^{-1}$.

COROLLARY 6.6. *Let A, B be two proper subsets of be a finite group G such that $B \subset A$ and $B = B^{-1}$. Then either $|A \cup (AB)| \geq |A| + |B|$ or there is $b \in B$ such that $\langle b \rangle$ is a subset of $A \cup (AB)$.*

The proof is similar to the proof of Corollary 6.4.

THEOREM 6.7. *For every $\varepsilon > 0$ and $k > 1$, there is some natural number n_0 such that for every $n > n_0$, and every subset $A \subset \mathbb{Z}_n$ satisfying*

$$|A| > \left(\frac{1}{k} + \varepsilon\right) n,$$

there is a non-zero element of A all of the multiples of which can be expressed as a sum of a subset of A of cardinality at most k.

PROOF. Let n_0 be such that $(1+\sqrt{3(k-2)})r(\mathbb{Z}_n) < \varepsilon n - 1$, for all $n > n_0$. This is possible by Theorem 2.D. Assume that

$$|A| > \left(\frac{1}{k} + \varepsilon\right)n.$$

By Alon's Theorem 2.F, there is $B \subset A\backslash 0$ such that $|B| \geq \lceil n/k \rceil$ with the following property:

For all j with $1 \leq j \leq k$ and all $x_1, \ldots, x_j \in B$, there exists a subset C of A with

$$|C| \leq k \quad \text{and} \quad \sum_{y \in C} y = x_1 + \cdots + x_j. \tag{1}$$

Consider the Cayley graph $X = \mathrm{Cay}(\langle B\rangle, B)$. By Theorem 5.5 there is $b \in B\backslash 0$ such that $H = \langle b\rangle$ is well connected in X. Let $x \in H$. By Lemma 5.1, x has a factorization with respect to B with length no more than $\lceil |\langle B\rangle|/|B| \rceil \leq \lceil n/|B| \rceil \leq k$. By (1), there exists a subset C of A with $|C| \leq k$ and $\sum_{y \in C} y = x$. □

THEOREM 6.8. *For every $\varepsilon > 0$ and $k > 1$, there is some natural number n_0 such that for every abelian group G with odd order at least n_0, and for every subset A of G satisfying*

$$|A| > \left(\frac{1}{k} + \varepsilon\right)|G|,$$

there is a non-zero element of A all of the multiples of which can be expressed as a sum of a subset of A of cardinality at most k.

The proof is the same as for Proposition 6.7 except that it uses Theorem 2.E instead of Theorem 2.D.

Theorem 6.7 implies the following result, proved by Alon [2].

THEOREM 6.9. *For every $\varepsilon > 0$ and $k > 1$, there is some natural number n_0 such that for every prime number $p > n_0$, and every subset $A \subset \mathbb{Z}_p$ satisfying*

$$|A| > \left(\frac{1}{k} + \varepsilon\right)p,$$

there is a non-zero element of A all of the multiples of which can be expressed as a sum of a subset of A of cardinality at most k.

REFERENCES

1. N. Alon, Subset sums, *J. Number Theory*, **27** (1987), 196–205.
2. N. Alon, private communication.
3. T. C. Brown and J. P. Buhler, A density version of a geometric Ramsey Theorem, *J. Combin. Theory, Ser. A*, **32** (1982), 20–34.
4. A. Cauchy, Recherches sur les nombres, *J. Ecole Polytechnique*, **9** (1813), 99–116.
5. I. Chowla, A theorem in the additive theory of numbers, *Proc. Natl. Acad. Sci. U.S.A.*, (1938), 160–164.
6. H. Davenport, On the addition of residue classes, *J. Lond. Math. Soc.*, **10** (1935), 30–32.
7. Y. O. Hamidoune, Sur les atomes d'un graphe orienté, *C. R. Acad. Sci. Paris*, **A284** (1977), 1253–1256.
8. Y. O. Hamidoune, Quelques problèmes de connexité dans les graphes orientés, *J. Combin. Theory, Ser. B*, **30** (1981), 1–10.

9. Y. O. Hamidoune, An application of connectivity theory in graphs to factorization of elements in groups, *Europ. J. Combin.*, **2** (1981), 108–112.
10. Y. O. Hamidoune, On the connectivity of Cayley digraphs, *Europ. J. Combin.*, **5** (1984), 309–312.
11. Y. O. Hamidoune, Sur la séparation dans les graphes de Cayley Abeliens, *Discr. Math.*, **55** (1985), 323–326.
12. McCuig, A simple proof of Menger's theorem, *J. Graph Theory*, **8** (1984), 427–429.
13. K. Roth, On certain sets of integers, *J. Lond. Math. Soc.*, **28** (1953), 104–109.
14. P. Scherk, Distinct elements in set of sums, *Am. Math. Monthly*, **62** (1955), 46–47.
15. J. C. Shepherdson, on the addition of elements of a sequence, *J. Lond. Math. Soc.*, **22** (1947), 85–88.

Received 11 October 1990 and accepted 30 November 1990

YAHYA OULD HAMIDOUNE
Université P. et M. Curie, UER 48, E. R. Combinatoire,
4 Place Jussieu, 75230 Paris, France