Combinatorics, Probability and Computing (2011) 20, 855–865. © Cambridge University Press 2011
doi:10.1017/S0963548311000459

Counting Certain Pairings in Arbitrary Groups

Y. O. HAMIDOUNE

Université Pierre et Marie Curie (Paris 6), Institut de Mathématiques de Jussieu,
Combinatoire et Optimisation, Case 189, 4 Place Jussieu, 75005 Paris, France

Received 13 December 2008; revised 8 September 2011; first published online 11 October 2011

In this paper, we study certain pairings which are defined as follows: if A and B are finite subsets of an arbitrary group, a *Wakeford–Fan–Losonczy pairing* from B onto A is a bijection $\phi : B \to A$ such that $b\phi(b) \notin A$, for every $b \in B$. The number of such pairings is denoted by $\mu(B, A)$.

We investigate the quantity $\mu(B, A)$ for A and B, two finite subsets of an arbitrary group satisfying $1 \notin B$, $|A| = |B|$, and the fact that the order of every element of B is $\geqslant |B| + 1$. Extending earlier results, we show that in this case, $\mu(B, A)$ is never equal to 0. Furthermore we prove an explicit lower bound on $\mu(B, A)$ in terms of $|B|$ and the cardinality of the group generated by B, which is valid unless A and B have a special form explicitly described. In the case $A = B$, our bound holds unless B is a translate of a progression.

1. Introduction

Let A and B be finite subsets of a (multiplicatively denoted) group G with $|A| = |B|$. A *Wakeford–Fan–Losonczy pairing* from B onto A is a bijection $\phi : B \to A$ such that $b\phi(b) \notin A$, for every $b \in B$. The number of distinct such pairings from B onto A will be denoted by $\mu(B, A)$.

Our pairings are dual to pairings used in the literature [4, 17, 2]. The two notions are equivalent up to replacing the group by its opposite group, or replacing (A, B) by (A^{-1}, B^{-1}). With this change of notation, isoperimetric theorems – which are central tools in this article – apply more quickly. Fan and Losonczy [4] introduced this notion of pairings in the group $\mathbb{Z}^n$ in connection with an old problem of Wakeford [24] related to canonical forms for symmetric tensors.

Let us define a *prime* group as a group having no proper finite subgroup. By elementary group theory, a group is a prime group if and only if it is a torsion-free group or if it has prime order.

In the abelian case, Losonczy [17] proved that if A and B are finite subsets of a prime abelian group, have the same cardinality and $1 \notin B$, then $\mu(B, A) \neq 0$. In the non-abelian case, Eliahou and Lecouvey [2] proved that if B is a finite subset of a group such that $1 \notin B$, then $\mu(B, B) \neq 0$.

Two remarks on these results are worth mentioning. First, the assumption $1 \notin B$ is obviously a necessary condition for the existence of at least one Wakeford–Fan–Losonczy pairing. Second, if one considers a proper finite subgroup H of some group G and $\beta \notin H$ and finally defines $B = (H \setminus \{1\}) \cup \{\beta\}$, it is readily seen that no Wakeford–Fan–Losonczy pairing $\phi : B \to H$

https://doi.org/10.1017/S0963548311000459 Published online by Cambridge University Press

can exist, since in this case one should have $b \notin H$ for all b in B, which is a contradiction since H has at least two elements. This observation made by Losonczy in [17] shows that in a non-prime group, there exist pairs of finite subsets A and B with the same cardinality such that $1 \notin B$, and $\mu(B, A) = 0$. Such a fact cannot hold in prime groups, by the result mentioned above, and justifies this restriction in Losonczy's result.

The two above-mentioned results are proved using some standard addition theorems that we now recall. Let A and B be finite subsets of a group G. Kneser's theorem [16] states that $|AB| \geqslant |A| + |B| - 1$ if G is abelian and if AB is aperiodic. The Scherk–Kemperman theorem states that $|AB| \geqslant |A| + |B| - 1$ if $A \cap B^{-1} = \{1\}$. This result was proved first by Scherk [23] for abelian groups and by Kemperman [15] for arbitrary groups. As observed in [2], the existence of a Wakeford–Fan–Losonczy pairing from a set onto itself is related to the Scherk–Kemperman theorem. In the non-abelian case, a result due to Olson [20] states that $|AB| \geqslant |A| + |B| - |H|$, where H is a subgroup depending on A and B. This last result is related to a result proved independently, and shortly before, by the author in [7]. Developments of this last result are known as isoperimetric results and will be central in this paper. We present it now.

The isoperimetric approach was developed by the author, notably in [7, 9, 8, 10, 13, 14]. Let us introduce briefly some terminology of this method which is needed to state our results.

Let S be a finite subset of a group G with $1 \in S$. The *kth connectivity* of S is defined as the quantity

$$\kappa_k(S) = \min\{|(XS) \setminus X| : \infty > |X| \geqslant k,\ X \subset \langle S\rangle \text{ and } |XS| \leqslant |\langle S\rangle| - k\},$$

where we denote by $\langle X\rangle$ the subgroup generated by a subset X of G and take the convention that $\min \emptyset = |\langle S\rangle| - k + 1$. We shall say that S is a *Cauchy subset* if $\kappa_1(S) = |S| - 1$ and that S is a *Vosper subset* if $\kappa_2(S) \geqslant |S|$.

Reformulating, S is a Cauchy subset if and only if, for every $X \subset \langle S\rangle$ with $|X| \geqslant 1$,

$$|XS| \geqslant \min\big(|\langle S\rangle|, |X| + |S| - 1\big),$$

while S is a Vosper subset if and only if, for every $X \subset \langle S\rangle$ with $|X| \geqslant 2$,

$$|XS| \geqslant \min\big(|\langle S\rangle| - 1, |X| + |S|\big).$$

Finally, a non-empty subset S of a group, not containing 1, will be called a *Chowla subset* if the order of every element of S is $\geqslant |S| + 1$. The notion of a Chowla subset, introduced by the author in [8] as a relaxation of Chowla's condition [1] in cyclic groups, allows one to extend additive properties of prime groups to a larger class of subsets in arbitrary groups.

The general philosophy is that existence of pairings is related to the Cauchy property while Vosper's property allows one to give a lower bound for the number of distinct pairings. We shall investigate pairings of a Chowla subset B onto an arbitrary A and obtain a lower bound for the number of distinct pairings in this case.

We now present the organization of the paper. Section 2 contains essentially known results. Section 2.1 contains the König–Hall theorem and its particular formulation in what we call the Wakeford–Fan–Losonczy graph. Section 2.2 recalls the Erdős–Heilbronn averaging argument needed to study this object. Section 2.3 presents some aspects of the isoperimetric formalism.

https://doi.org/10.1017/S0963548311000459 Published online by Cambridge University Press

In Section 3, we prove an inverse theorem for cofinite sets. As an application, we obtain the following result.

Theorem 1.1. *Let B be a finite Chowla subset of an arbitrary group G. If A is a subset of G with $|A| = |B|$, then $\mu(B, A) \neq 0$.*

For a given group G, we denote

$$m(G) = \min\{|M| : M \text{ is a finite subgroup of } G, \text{ with } 2 \leqslant |M| < |G|\},$$

where $\min \emptyset = \infty$. In particular $m(G) = \infty$ if G is a prime group. With this notation, Theorem 1.1 immediately implies the following corollary.

Corollary 1.2. *Let B be a finite subset of an arbitrary group G with $1 \notin B$ and let A be a subset of G with $|A| = |B|$. If $|B| < m(G)$, then $\mu(B, A) \neq 0$.*

Applied to groups with prime order, the last result reduces to a result of Losonczy [17]. Also in the case of torsion-free groups, it implies Eliahou and Lecouvey's result [2] generalizing results of Wakeford [24] and Losonczy [17] in the abelian case.

In Section 4, we refine our study. In the case of Chowla subsets, we can obtain an explicit lower bound on $\mu(B, A)$. However, one has to take care of specific situations where $\mu(B, A)$ cannot be lower-bounded efficiently. Indeed, if for instance P denotes the r-progression $P = \{1, r, \cdots, r^j\}$ (for some $r \in G$ and positive integer j smaller than the order of r), then an inductive argument shows easily that there is a unique Wakeford–Fan–Losonczy pairing from rP onto P, given by $\phi : r^s \mapsto r^{j+1-s}$ $(1 \leqslant s \leqslant j+1)$. Thus in this case $\mu(rP, P) = 1$.

The structure of a progression appears in a natural way in the present study. A subset of a given group G of the form $\{ar^s : 1 \leqslant s \leqslant j\}$ (resp. $\{r^s a : 1 \leqslant s \leqslant j\}$) (with $a, r \in G$) will be called a *left r-progression* (resp. a *right r-progression*). A set which is both a left and a right r-progression is simply called an *r-progression*. We may not need to specify the ratio (that is, r) of the progression. Notice that a left or right progression containing 1 is a progression, therefore these two notions coincide in this case and, for this reason, we shall formulate some results using translate copies of sets.

Our forthcoming theorem shows that, except in some specific situations, there is typically a much larger number of Wakeford–Fan–Losonczy pairings.

Theorem 1.3. *Let B be a finite Chowla subset of an arbitrary group G. Let A be a subset of G with $|A| = |B|$. Then, one of the following holds:*

(i) $\mu(B, A) \geqslant \min\{\frac{|B|+1}{3}, \frac{|B|(|\langle B\rangle|-|B|-1)}{2|\langle B\rangle|-|B|-4}\}$,
(ii) *there is an $a \in A$ such that $|Aa^{-1} \cap B| = |B| - 1$,*
(iii) *there is an $a \in A$ such that Aa^{-1} is a progression.*

Our final statement is a consequence of Theorem 1.3.

https://doi.org/10.1017/S0963548311000459 Published online by Cambridge University Press

Corollary 1.4. *Let B be a finite Chowla subset. If there is no $b \in B$ such that Bb^{-1} is a progression, then*

$$\mu(B,B) \geqslant \min\left\{\frac{|B|+1}{3}, \frac{|B|(|\langle B\rangle| - |B| - 1)}{2|\langle B\rangle| - |B| - 4}\right\}.$$

2. Preliminaries

2.1. Matchings

Let V and W be two sets and let $\mathcal{R}$ be a subset of $V \times W$. For $x \in V$, we write $\mathcal{R}(x)$ for those $y \in W$ such that $(x,y) \in \mathcal{R}$. For $X \subset V$, we write $\mathcal{R}(X)$ for those $y \in W$ such that $(x,y) \in \mathcal{R}$ for at least one x in V. Finally we define $\mathcal{R}^{-1} = \{(y,x) \in W \times V : (x,y) \in \mathcal{R}\}$. We shall write

$$\Delta(\mathcal{R}) = \max\{|\mathcal{R}(x)| : x \in V\}.$$

A *selection* of $\mathcal{R}$ is a mapping $\mathcal{S} : V \to W$ such that $(x, \mathcal{S}(x)) \in \mathcal{R}$, for every $x \in V$. If $|V| = |W|$, a bijective selection of $\mathcal{R}$ is called a *matching* of $\mathcal{R}$. The number of matchings of $\mathcal{R}$ will be denoted by $\mu(\mathcal{R})$.

We shall use the next two known results for which we refer to [18].

Theorem 2.1 (König–Hall theorem). *Let $\mathcal{R}$ be a subset of $V \times W$, where V and W are two sets with the same cardinality. Then $\mathcal{R}$ has a matching if and only if $|\mathcal{R}(Y)| \geqslant |Y|$, for every subset Y of V.*

An easy consequence of the König–Hall theorem is the following result observed by Hetyei.

Corollary 2.2. *Let $\mathcal{R}$ be a subset of $V \times W$, where V and W are two sets with the same cardinality such that $|\mathcal{R}(Y)| \geqslant |Y| + 1$, for every proper subset Y of V. Then every $(x,y) \in \mathcal{R}$ lies in some matching of $\mathcal{R}$. In particular, $\mu(\mathcal{R}) \geqslant \max\{\Delta(\mathcal{R}), \Delta(\mathcal{R}^{-1})\}$.*

Some applications of matching theory may be found in the book by Lovász and Plummer [18]. We also mention applications of Theorem 2.1 and Corollary 2.2 by Fournier [5] to planar tilings.

We now apply matching theory to our context. We consider an arbitrary group G. For a subset $X \subset G$, we shall write

$$\overline{X} = G \setminus X, \quad \tilde{X} = X \cup \{1\} \quad \text{and} \quad X^{-1} = \{x^{-1} : x \in X\}.$$

Let A and B be two finite subsets of G. We call

$$\mathcal{R} = \mathcal{R}(B,A) = \{(b,a) \in B \times A \mid ba \notin A\}$$

the *Wakeford–Fan–Losonczy graph* of the pair (A,B). It is clear that a Wakeford–Fan–Losonczy pairing from B onto A is just a matching of the corresponding Wakeford–Fan–Losonczy graph. Thus

$$\mu(B,A) = \mu(\mathcal{R}).$$

https://doi.org/10.1017/S0963548311000459 Published online by Cambridge University Press

For every $b \in B$, we have $\mathcal{R}(b) = A \cap (b^{-1}\overline{A}) = A \setminus (b^{-1}A)$. In particular, it follows that

$$|\mathcal{R}(b)| = |A \setminus (b^{-1}A)| = |bA \setminus A|, \tag{2.1}$$

a quantity which will be studied in the next subsection.

For every $X \subset B$, we have that $\mathcal{R}(X) = A \cap (X^{-1}\overline{A})$. Since

$$\mathcal{R}(X) = A \cap (X^{-1}\overline{A}) = (X^{-1}\overline{A}) \setminus \overline{A} = ((\tilde{X}^{-1})\overline{A}) \setminus \overline{A},$$

Hall's condition in this graph takes the following form: for every $X \subset B$, $|X| \leqslant |(\tilde{X})^{-1}\overline{A}) \setminus \overline{A}|$. In particular, by the König–Hall theorem (Theorem 2.1) and Corollary 2.2 we have the following result.

Lemma 2.3. *Let B be a finite subset of a group G with $1 \notin B$ and let A be a subset of G with $|A| = |B|$. Let $\mathcal{R} \subset B \times A$ be the corresponding Wakeford–Fan–Losonczy graph. Then the following two assertions hold:*

(i) *$\mu(B, A) \neq 0$ if and only if, for every $X \subset B$, $|X| \leqslant |(\overline{A^{-1}}\tilde{X}) \setminus \overline{A^{-1}}|$,*
(ii) *if $\mu(B, A) < \Delta(\mathcal{R})$, then there exists a proper subset $X \subset B$ satisfying*

$$|X| \geqslant |(\overline{A^{-1}}\tilde{X}) \setminus \overline{A^{-1}}|.$$

2.2. The Erdős–Heilbronn averaging argument

Let G be a group, $B \subset G$ and $x \in G$. The Erdős–Heilbronn function λ is defined as

$$\lambda_B(x) = |(Bx) \setminus B|.$$

Erdős and Heilbronn introduced this function in the abelian case and proved its submodularity [3]. Olson generalized it to the non-abelian case.

We need two properties of this function.

Lemma 2.4 (Olson's theorem [19]). *Let S and T be two non-empty subsets of a group G such that $1 \notin S$. Then,*

$$\lambda_T(x) + \lambda_T(y) \geqslant \lambda_T(xy), \tag{2.2}$$

$$\sum_{x \in S} \lambda_T(x) \geqslant |T|(|S| - |T| + 1). \tag{2.3}$$

The following lemma will be used later to show that the maximal degree of a Wakeford–Fan–Losonczy graph cannot be too small.

Lemma 2.5. *Let S and T be two non-empty finite subsets of a group G with $1 \notin S$. Then there is an $x \in S$ such that*

$$\lambda_T(x) \geqslant \min\left\{\frac{|T|(|S| + \kappa_2 - |T| + 1)}{|S| + 2\kappa_2}, \frac{|T|(|\langle S\rangle| - |T| - 1)}{2|\langle S\rangle| - |S| - 4}\right\},$$

where $\kappa_2 = \kappa_2(\tilde{S})$.

https://doi.org/10.1017/S0963548311000459 Published online by Cambridge University Press

In particular, if $\kappa_2 \geqslant |S| = |T|$, then there is an $x \in S$ such that

$$\lambda_T(x) \geqslant \min\left\{\frac{|S|+1}{3}, \frac{|S|(|\langle S\rangle| - |S| - 1)}{2|\langle S\rangle| - |S| - 4}\right\}. \tag{2.4}$$

Proof. Put $\alpha = \max\{\lambda_T(x) : x \in S\}$ and $q = |\langle S\rangle|$. By the definition of κ_2, we have $|\tilde{S}^2| \geqslant \min(q-1, 1+|S|+\kappa_2)$. Take a subset C of $\tilde{S}^2$ such that $1 \notin C$, $S \subset C$ and $|C| = \min(q-2, |S|+\kappa_2)$.

By (2.3), (2.2) and the fact that an element of C is a product of at most two elements of S, we get

$$\begin{aligned} |T|(|C| - |T| + 1) &\leqslant \sum_{x\in C} \lambda_T(x) \\ &= \sum_{x\in S} \lambda_T(x) + \sum_{x\in C\setminus S} \lambda_T(x) \\ &\leqslant \alpha|S| + 2\alpha(|C| - |S|) \\ &= \alpha(2|C| - |S|). \end{aligned}$$

Thus we obtain

$$\alpha \geqslant \frac{|T|(|C| - |T| + 1)}{2|C| - |S|}.$$

In the case where $|S| + \kappa_2 \leqslant q - 2$, we have $|C| = |S| + \kappa_2$ and hence

$$\alpha \geqslant \frac{|T|(|S| + \kappa_2 - |T| + 1)}{|S| + 2\kappa_2}.$$

Assume now that $|S| + \kappa_2 > q - 2$; then $|C| = q - 2$ and hence

$$\alpha \geqslant \frac{|T|(q - |T| - 1)}{2q - |S| - 4}.$$

□

2.3. Isoperimetric preliminaries

Let S and T be two subsets of a group G with $1 \in S$. We define

$$T^S = G \setminus (TS) \quad \text{and} \quad \partial_S(T) = (TS) \setminus T.$$

Clearly

$$T \cup T^S \cup \partial_S(T)$$

is a partition of G. We shall write

$$\partial_S^-(T) = (TS^{-1}) \setminus T.$$

Notice that one has $\partial_S^-(T^S) \cap T = \emptyset$, since otherwise there exist $z \in T^S$ and $y \in S$ such that $zy^{-1} = x \in T$, and hence $z = xy \in TS$, a contradiction. Hence, since $\partial_S^-(T^S) \subset G \setminus T^S = TS$, we have

$$\partial_S^-(T^S) \subset \partial_S(T). \tag{2.5}$$

https://doi.org/10.1017/S0963548311000459 Published online by Cambridge University Press

This last observation, which is used extensively in the isoperimetric method, contains a useful duality.

Recall the following result.

Theorem 2.6 ([7, 10]). *Let S be a finite subset of a group, containing 1. Then there is a finite subgroup $L \neq \langle S\rangle$ generated by a subset of S such that $\kappa_1(S) = \min(|LS| - |L|, |SL| - |L|)$.*

Corollary 2.7 (Proposition 2.8 in [8]). *For any finite Chowla subset S, one has $\kappa_1(\tilde{S}) = |S|$.*

Proof. By Theorem 2.6 applied to $\tilde{S}$, for some finite subgroup $L \neq \langle \tilde{S}\rangle = \langle S\rangle$, generated by a non-empty subset of S, we have $\kappa_1(\tilde{S}) = \min(|L\tilde{S}| - |L|, |\tilde{S}L| - |L|)$.

Notice first the obvious inequality $\kappa_1(\tilde{S}) \leqslant |\tilde{S}| - 1 = |S|$, which holds by definition (taking $X = \{1\}$).

If $|L| \geqslant 2$, since $1 \in \tilde{S}$ and $L \neq \langle \tilde{S}\rangle$, $\tilde{S}$ meets at least two L-cosets and we must therefore have

$$\min(|L\tilde{S}|, |\tilde{S}L|) \geqslant 2|L|.$$

Thus $\kappa_1(\tilde{S})$ would be at least $|L|$; but L contains at least one element different from 1 which has an order $\geqslant |S| + 1$ by definition of a Chowla set. This would imply $\kappa_1(\tilde{S}) \geqslant |S| + 1$, a contradiction.

Therefore $|L| = 1$ and $\kappa_1(\tilde{S}) = |\tilde{S}| - 1 = |S|$. □

We also need the following more precise result.

Theorem 2.8 (Theorem 3.2 in [8]). *Let S be a finite Chowla subset. Then $\tilde{S}$ is either a Vosper subset or a progression.*

3. An inverse theorem for cofinite subsets

Inverse theory (including the isoperimetric approach) deals only with finite sets. In this section, we derive an inverse theorem for cofinite sets.

Proposition 3.1. *Let S be a finite Cauchy subset of a group G with $1 \in S$. Let T be a cofinite subset of G with $TS \neq G$ and $|\overline{T}| \leqslant |\langle S\rangle| - 1$.*

Then

$$|\partial_S(T)| \geqslant |S| - 1.$$

Assuming moreover that S satisfies $|\partial_S(T)| = |S| - 1$, we have

$$T^S(T^S)^{-1} \subset \langle S\rangle, \tag{3.1}$$

$$(T^S)S^{-1} = \overline{T}, \tag{3.2}$$

$$|(T^S)S^{-1}| = |T^S| + |S| - 1. \tag{3.3}$$

Proof. Put $Z = T^S$ and $H = \langle S\rangle$. Take a left-decomposition $Z = Z_1 \cup \cdots \cup Z_j$ of Z modulo H (H-tiling), where the $Z_i = z_iH \cap Z$ (for some $z_i \in Z$) are the j (j a positive integer) non-empty disjoint intersections of left H-cosets with Z.

https://doi.org/10.1017/S0963548311000459 Published online by Cambridge University Press

By (2.5), we obtain

$$\begin{aligned} Z_iS^{-1} &\subset ZS^{-1} \\ &= Z \cup \partial_S^-(Z) \\ &\subset Z \cup \partial_S(T) \\ &= \overline{T}, \end{aligned}$$

and hence $|Z_iS^{-1}| \leqslant |\overline{T}| \leqslant |H| - 1$. We then deduce, using the definition of a Cauchy set, that

$$|Z_iS^{-1}| = |(z_i^{-1})Z_iS^{-1}| \geqslant \min(|H|, |Z_i| + |S| - 1) = |Z_i| + |S| - 1.$$

Summing these j contributions, we obtain

$$|ZS^{-1}| = \sum_{1 \leqslant i \leqslant j} |Z_iS^{-1}| \geqslant |Z| + j(|S| - 1).$$

From this bound and (2.5), it follows that

$$j(|S| - 1) \leqslant |ZS^{-1}| - |Z| = |\partial_S^-(Z)| \leqslant |\partial_S(T)|. \tag{3.4}$$

In particular, $j \geqslant 1$ implies

$$|\partial_S(T)| \geqslant |S| - 1$$

and proves the first assertion.

From now on, we additionally assume that $|\partial_S(T)| = |S| - 1$. By (3.4), and since $|S| \geqslant 2$, we obtain $j = 1$ and

$$|S| - 1 = |\partial_S^-(Z)| = |\partial_S(T)|. \tag{3.5}$$

The fact that $j = 1$ proves that Z is included in a unique H-coset. So does ZZ^{-1}. Since $1 \in ZZ^{-1}$, we obtain

$$ZZ^{-1} \subset H,$$

that is, (3.1).

By (3.5), we infer in particular

$$|(T^S)S^{-1}| = |T^S| + |S| - 1,$$

proving (3.3).

Finally, by (3.5) and (2.5) we get $\partial_S^-(Z) = \partial_S(T)$, and therefore obtain

$$(T^S)S^{-1} = T^S \cup \partial_S^-(T^S) = T^S \cup \partial_S(T) = \overline{T},$$

proving (3.2). □

We can now show that Chowla subsets behave nicely with respect to matchability, and give the proof of Theorem 1.1.

Proof of Theorem 1.1. Let X be an arbitrary non-empty subset of B and define $H = \langle X \rangle$ and $S = \tilde{X}$. Clearly, X is also a Chowla subset and each of its elements has an order at

https://doi.org/10.1017/S0963548311000459 Published online by Cambridge University Press

least $|B|+1$, therefore $|H| \geqslant |B|+1$. By Corollary 2.7, $\kappa_1(S) = |S|-1$ and S is a Cauchy subset containing 1.

We define the cofinite set $T = (\overline{A})^{-1}$ and check that $|\overline{T}| = |A| = |B| \leqslant |H|-1$. We are therefore in a position to apply Proposition 3.1, which yields

$$|\overline{A^{-1}}\tilde{X} \setminus \overline{A^{-1}}| = |\partial_S(T)| \geqslant |S|-1 = |X|.$$

By assertion (i) of Lemma 2.3, $\mu(B,A) \neq 0$. □

4. Distinct matchings

Vosper's property implies a bound on the number of distinct matchings. We shall now illustrate this relation in the easier case of Chowla subsets by giving the proof of Theorem 1.3.

Proof of Theorem 1.3. Define $q = |\langle B\rangle|$. Suppose that (i) is not satisfied. By Lemma 2.5, (2.1) and the definition of the Erdős–Heilbronn function λ, this implies

$$\mu(B,A) < \Delta(\mathcal{R})$$

if $\mathcal{R}$ denotes the corresponding Wakeford–Fan–Losonczy graph.

By Lemma 2.3, for some proper subset X of B, we have $|(\overline{A^{-1}}\tilde{X}) \setminus \overline{A^{-1}}| \leqslant |X|$. This can be rephrased as

$$|\partial_S(T)| \leqslant |S|-1 \tag{4.1}$$

if we define

$$S = \tilde{X}, \quad T = \overline{A^{-1}}, \quad H = \langle X\rangle = \langle S\rangle, \quad \text{and} \quad Z = T^S.$$

We choose $z \in Z$.

Again, X is also a Chowla subset and each of its elements has an order at least $|B|+1$, therefore $|H| \geqslant |B|+1$. By Corollary 2.7, $\kappa_1(S) = |S|-1$ and S is a Cauchy subset containing 1. We notice that $TS \neq G$, for otherwise $\overline{A^{-1}}\tilde{X} = G$, which would imply, by definition of X, $|A| \leqslant |X| < |B|$, a contradiction. By the first assertion of Proposition 3.1, $|\partial_S(T)| \geqslant |S|-1$ and, with (4.1), we obtain

$$|\partial_S(T)| = |S|-1,$$

and we are in a position to apply the last three results of Proposition 3.1. In particular, by (3.2),

$$A^{-1} = \overline{T} = ZS^{-1}. \tag{4.2}$$

Notice that $z \in A^{-1}$.

Assume first that $|Z| = 1$, and hence $Z = \{z\}$. We clearly have $Az = S$. Thus $|A| = |S| = |X|+1$, and hence $|X| = |B|-1$. Therefore $|Az \cap B| = |S \cap B| = |\tilde{X} \cap B| = |X| = |B|-1$, and (ii) holds.

Assume now $|Z| \geqslant 2$. By Theorem 2.8, either S is an r-progression for some element $r \in G$, or S is a Vosper subset.

https://doi.org/10.1017/S0963548311000459 Published online by Cambridge University Press

If S is an r-progression, for some element $r \in G$, then, by (3.3) and (4.2), $|Z| + |S| - 1 = |SZ^{-1}| = |A| \leqslant |H| - 1$. It follows, using Lemma 3.1 of [8], that $Z^{-1}z$ is a progression and hence $SZ^{-1}z = Az$ is a progression. Thus (iii) holds.

If S is a Vosper subset, then $|X| = |S| - 1 \geqslant 2$, since a subset of size 2 is not a Vosper subset. Choose $r \in X$. By (3.3), $|SZ^{-1}| = |Z| + |S| - 1 = |A| \leqslant |H| - 1$. Since S is a Vosper subset of H, we must have $|A| = |SZ^{-1}| = |H| - 1$. By (3.1), $A \subset Hz^{-1}$, and hence $|Az \cap H| = |H| - 1$. But $|\langle r\rangle| \geqslant |A| + 1 = |H|$, and hence $H = \langle r\rangle$. Since H is cyclic, any subset of H with size $|H| - 1$ is a progression. Thus Az is a progression and (iii) holds. □

The corollary then follows.

Proof of Corollary 1.4. Assume the conclusion of the statement fails. Then, by Theorem 1.3, there is a $b \in B$ such that $|Bb^{-1} \cap B| = |B| - 1$. Since $b \neq 1$, we have $|B\{1, b\}| = |B| + 1$. Since $|B|$ is less than the order of b, B is a progression composed of powers of b. Thus Bb^{-1} is a progression. □

Note

Yahya ould Hamidoune [21, 22] passed away before he could prepare a revised version of this article. The present revised version was prepared by A. Plagne with the aim of improving readability, keeping in mind Hamidoune's idiosyncrasies. The original submitted version [12] can still be found on `arXiv`.

References

[1] Chowla, S. (1935) A theorem on the addition of residue classes: Applications to the number $\Gamma(k)$ in Waring's problem. *Proc. Indian Acad. Sci.* **2** 242–243.
[2] Eliahou, S. and Lecouvey, C. (2008) Matchings in arbitrary groups. *Adv. Appl. Math.* **40** 219–224.
[3] Erdős, P. and Heilbronn, H. (1964) On the addition of residue classes mod p. *Acta Arith.* **9** 149–159.
[4] Fan, C. K. and Losonczy, J. (1996) Matchings and canonical forms in symmetric tensors. *Adv. Math.* **117** 228–238.
[5] Fournier, J. C. (2003) Combinatorics of perfect matchings in plane bipartite graphs and application to tilings. *Theoret. Comput. Sci.* **303** 333–351.
[6] Hall, P. (1935) On representatives of subsets. *J. London Math. Soc.* **10** 26–30.
[7] Hamidoune, Y. O. (1984) On the connectivity of Cayley digraphs. *Europ. J. Combin.* **5** 309–312.
[8] Hamidoune, Y. O. (1996) An isoperimetric method in additive theory. *J. Algebra* **179** 622–630.
[9] Hamidoune, Y. O. (1997) On subsets with a small sum in abelian groups I: The Vosper property. *Europ. J. Combin.* **18** 541–556.
[10] Hamidoune, Y. O. (1999) On small subset product in a group. In *Structure Theory of Set-Addition*, Vol. 258 of *Astérisque*, pp. 281–308.
[11] Hamidoune, Y. O. (2000) Some results in additive number theory I: The critical pair theory. *Acta Arith.* **96** 97–119.
[12] Hamidoune, Y. O. (2008) On group bijections ϕ with $\phi(B) = A$ and $\forall a \in B, a\phi(a) \notin A$. `arXiv:0812.2522`.
[13] Hamidoune, Y. O. Hyper-atoms and the Kemperman's critical pair theory, `arXiv.0708.3581`.
[14] Hamidoune, Y. O. Hyper-atoms applied to the critical pair theory. Submitted. `arXiv:1102.2099v1`
[15] Kemperman, J. H. B. (1956) On complexes in a semigroup. *Nederl. Akad. Wetensch. Proc. Ser. A* **59** 247–254.

https://doi.org/10.1017/S0963548311000459 Published online by Cambridge University Press

[16] Kneser, M. (1953) Abschätzung der asymptotischen Dichte von Summenmengen. *Math. Z.* **58** 459–484.
[17] Losonczy, J. (1998) On matchings in groups. *Adv. Appl. Math.* **20** 385–391.
[18] Lovász, L. and Plummer, M. D. (1986) Matching theory. *Ann. Discrete Math.* **29**.
[19] Olson, J. E. (1975/76) Sums of sets of group elements. *Acta Arith.* **28** 147–156.
[20] Olson, J. E. (1984) On the sum of two sets in a group. *J. Number Theory* **18** 110–120.
[21] Plagne, A. (2011) Yahya ould Hamidoune, grand Mauritanien, homme singulier, mathématicien d'exception. *Gaz. Math.* **129** 123–129.
[22] Plagne, A. (2011) Yahya ould Hamidoune, *the* Mauritanian mathematician. *Combin. Probab. Comput.* **20** 641–645.
[23] Scherk, P. and Moser, L. (1955) Advanced problems and solutions: Solutions, 4466. *Amer. Math. Monthly* **62** 46–47.
[24] Wakeford, E. K. (1918/1919) On canonical forms. *Proc. London Math. Soc.* **18** 403–410.

https://doi.org/10.1017/S0963548311000459 Published online by Cambridge University Press