

ON MATCHINGS IN GROUPS

JOZSEF LOSONCZY

ABSTRACT. A matching property conceived for lattices is examined in the context of an arbitrary abelian group. The Dyson e -transform and the Cauchy–Davenport inequality from additive number theory are used to establish the existence of matchings.

1. INTRODUCTION AND DEFINITIONS

Let G be a lattice (discrete additive subgroup of \mathbb{R}^n). Given m lattice points and m direction vectors from G , it is possible to pair the lattice points with the direction vectors so that the sum within each pair is not one of the given lattice points; moreover, this can be done in such a way that the pairing is uniquely determined by the lattice points, direction vectors and multiset of sums [1]. We explore in the present paper the extent to which the above matching property is satisfied by an arbitrary abelian group G .

In what follows, A and B will denote nonempty finite subsets of an additive abelian group G that satisfy $|A| = |B|$ and $0 \notin B$. A bijection $\pi: A \rightarrow B$ is called a *matching* if $a + \pi(a) \notin A$ for all $a \in A$. Given such a bijection π , we define $m_\pi: G \rightarrow \mathbb{Z}$ by $m_\pi(g) = \#\{a \in A \mid a + \pi(a) = g\}$, and we call π *acyclic* if for any matching $\tau: A \rightarrow B$ with $m_\tau = m_\pi$, we have $\tau = \pi$. Our goal is to identify conditions that guarantee the existence of matchings.

We will find it necessary to appeal to a few notions from additive number theory, in particular, the Dyson e -transform, the Cauchy–Davenport inequality and an addition theorem of Kneser. For a detailed treatment of these topics, see [8] or [9].

Given any subsets S, T of G , define $S + T = \{u \in G \mid u = s + t \text{ for some } s \in S \text{ and } t \in T\}$.

2. SYMMETRIC CASE

We obtain the following general result on matchings when A and B are equal.

Theorem 2.1. *Let G be an abelian group. Given any nonempty finite subset A of $G \setminus \{0\}$, there exists at least one matching $\pi: A \rightarrow A$.*

Proof. Let S be a nonempty subset of A . Define $U = \{a \in A \mid s + a \in A \text{ for all } s \in S\}$ and put $T = U \cup \{0\}$.

Case 1: $S + T = S$. Then S and T are disjoint. To see this, assume for contradiction the existence of some $s \in S \cap T$. Then $2s = s + s \in S + T = S$, $3s = 2s + s \in S + T = S$,

and, continuing in this way, $ns \in S$ for all positive integers n . Since S is finite and does not contain 0, this produces a contradiction.

Disjointedness of S and T implies $|S| + |U| \leq |A|$; hence $|S| \leq |A \setminus U|$. By P. Hall's marriage theorem, there exists a permutation π of A satisfying $a + \pi(a) \notin A$ for all $a \in A$.

Case 2: $S + T \neq S$. We may select $e \in S$ and $t \in T$ such that $e + t \notin S$. Define two sets $S(e)$ and $T(e)$ as follows:

$$S(e) = S \cup (e + T),$$

$$T(e) = T \cap (S - e).$$

The sets $S(e)$ and $T(e)$ satisfy the following four properties:

$$(1) \quad S(e) + T(e) \subseteq S + T,$$

$$(2) \quad |S(e)| + |T(e)| = |S| + |T|,$$

$$(3) \quad 0 \in T(e) \subseteq T,$$

$$(4) \quad |S(e)| > |S|.$$

Note that properties (1), (2) and (3) would hold for any $e \in G$ together with any finite subsets S and T of G such that $e \in S$ and $0 \in T$. Property (1) follows directly from the definition of the transformed sets $S(e)$, $T(e)$. Property (2) can be verified as follows: $|S(e)| = |S \cup (e + T)| = |S| + |T| - |S \cap (e + T)|$, and there is a bijection from $T \cap (S - e)$ to $S \cap (e + T)$ given by $u \mapsto u + e$. The sets $S(e)$, $T(e)$ are known as the Dyson e -transforms of S and T .

If $S(e) + T(e) \neq S(e)$, repeat the above procedure, replacing S with $S(e)$ and T with $T(e)$. Continuing in this way, since $S + T \subseteq A$, A is finite and the sets S , $S(e)$, \dots are strictly increasing in size, we eventually obtain sets S' , T' satisfying

$$S' + T' = S' \subseteq A,$$

$$|S'| + |T'| = |S| + |T|,$$

$$0 \in T' \subseteq T.$$

Since S' is finite and does not contain 0, we have $S' \cap T' = \emptyset$ (by the same argument as given in Case 1). Observing that S' and $T' \setminus \{0\}$ are contained in A , we obtain $|S'| + |T'| - 1 \leq |A|$. Therefore, $|S| + |U| = |S| + |T| - 1 = |S'| + |T'| - 1 \leq |A|$, whence $|S| \leq |A \setminus U|$. Appealing as in Case 1 to P. Hall's marriage theorem, we deduce the existence of a matching from A to itself. \square

Remark 2.2. We can reformulate Theorem 2.1 as follows: Let a_1, \dots, a_n be distinct nonzero elements of an abelian group G . Then at least one of the $n!$ diagonals of the matrix $\{a_i + a_j\}$ contains no a_i .

Remark 2.3. Our particular use of the Dyson e -transform in the proof of Theorem 2.1 follows [8, Lemma 1.5.2].

Remark 2.4. There may exist only one matching $\pi : A \rightarrow A$. Take, for example, $G = \mathbb{Z}$ and $A = \{1, 2, \dots, n\}$.

Remark 2.5. The issue of when an acyclic matching $A \rightarrow A$ exists will be treated in the fourth section of this paper. We mention here that acyclic matchings are not always available. For example, if $G = \mathbb{Z}/7\mathbb{Z}$ and $A = \{\bar{1}, \bar{2}, \bar{4}\}$, then there are exactly two matchings: $\pi : \bar{1} \mapsto \bar{2}, \bar{2} \mapsto \bar{4}, \bar{4} \mapsto \bar{1}$ and $\tau : \bar{1} \mapsto \bar{4}, \bar{2} \mapsto \bar{1}, \bar{4} \mapsto \bar{2}$. It is easy to see that $m_\pi = m_\tau$.

3. ASYMMETRIC CASE

In this section, we make use of the following addition theorem, whose proof can be found in [8] or [9]:

Theorem (Kneser). *Let G be an abelian group and S, T nonempty finite subsets. There exists a subgroup H of G such that*

$$\begin{aligned} S + T + H &= S + T, \\ |S + T| &\geq |S + H| + |T + H| - |H|. \end{aligned}$$

We say that G possesses the *matching property* if for every pair A, B of nonempty finite subsets satisfying $|A| = |B|$ and $0 \notin B$, there exists at least one matching from A to B .

Theorem 3.1. *An abelian group G possesses the matching property if and only if it is torsion-free or cyclic of prime order.*

Proof. The trivial group has the matching property and is torsion-free, so we may take $|G| \geq 2$ in what follows. Assume that G has the matching property, and let $g \in G \setminus \{0\}$. Suppose $0, g, \dots, ng$ are distinct, where n is any nonnegative integer (less than $|G| - 1$, if G is finite). There exists a matching from $A(n) = \{0, g, \dots, ng\}$ to $B(n) = \{g, h_1, \dots, h_n\}$, where h_1, \dots, h_n are (any) n distinct elements in $G \setminus \{0, g\}$. But this implies $(n+1)g \neq 0, g, \dots, ng$. It follows that G has no finite proper subgroups, and so is either torsion-free or cyclic of prime order.

Conversely, if G has no finite proper subgroups, then the theorem of Kneser stated above implies the following inequality, valid for all nonempty finite subsets S and T :

$$(5) \quad |S + T| \geq \min\{|G|, |S| + |T| - 1\}.$$

Let A and B be nonempty finite subsets of G satisfying $|A| = |B|$ and $0 \notin B$. Let $S \subseteq A$ be nonempty and define $U = \{b \in B \mid s + b \in A \text{ for all } s \in S\}$. Put $T = U \cup \{0\}$. Applying inequality (5) to S and T , and noting that $S + T \subseteq A$, we obtain $|B| = |A| \geq |S + T| \geq |S| + |T| - 1 = |S| + |U|$. Hence, $|B \setminus U| \geq |S|$. By P. Hall's marriage theorem, there exists a bijection $\pi : A \rightarrow B$ satisfying $a + \pi(a) \notin A$ for all $a \in A$. We conclude that G has the matching property. \square

Remark 3.2. When G is cyclic of prime order, inequality (5) appearing in the proof of Theorem 3.1 is known as the Cauchy–Davenport inequality. Cauchy [2] used it

to prove that given $a, b, c \in \mathbb{Z}/p\mathbb{Z}$, where p is prime and $a, b \neq 0$, the equation $ax^2 + by^2 = c$ has a solution in x, y from $\mathbb{Z}/p\mathbb{Z}$. Davenport [4, 5] later discovered the inequality for $\mathbb{Z}/p\mathbb{Z}$ independently, and published with it a different, but equivalent formulation.

Remark 3.3. In [6], \mathbb{R}^n was shown to possess the matching property by introducing an inner product and working with hyperplanes.

Theorem 3.1 implies that cyclic groups of prime or infinite order have the matching property. Concerning the other cyclic groups, we can at least say the following.

Proposition 3.4. *Let G be a nontrivial finite cyclic group. Suppose we are given nonempty subsets $A, B \subseteq G$ such that $|A| = |B|$ and every element of B is a generator of G . Then there exists at least one matching $\pi : A \rightarrow B$.*

Proof. Let S be a nonempty subset of A , define $U = \{b \in B \mid s+b \in A \text{ for all } s \in S\}$, and put $T = U \cup \{0\}$. By the theorem of Kneser stated above, there exists a subgroup H of G satisfying $S+T+H = S+T$ and $|S+T| \geq |S+H| + |T+H| - |H|$. Observe that $H \neq G$; otherwise, $S+T = S+T+H = S+T+G = G$, and since $S+T \subseteq A$, this gives $A = G$, contradicting the fact that A is a proper subset of G (A has the same size as B and $0 \notin B$).

Clearly, both H and T are contained in $T+H$; moreover, because every nonzero element of T is a generator and H is a subgroup unequal to G , we have $T \cap H = \{0\}$. It follows that $|T+H| \geq |T| + |H| - 1$. Combining this with the inequality $|S+T| \geq |S+H| + |T+H| - |H|$, we get $|S+T| \geq |S| + |T| - 1$. In sum, we have $|B| = |A| \geq |S+T| \geq |S| + |U|$, which implies $|B \setminus U| \geq |S|$. By P. Hall's marriage theorem, there exists a matching $\pi : A \rightarrow B$. \square

Remark 3.5. One can extract from the proof of Proposition 3.4 the following consequence of Kneser's theorem: suppose we are given nonempty subsets $S, T \subseteq \mathbb{Z}/n\mathbb{Z}$ such that $S+T \neq G$, $0 \in T$ and every element of $T \setminus \{0\}$ is a generator of $\mathbb{Z}/n\mathbb{Z}$. Then $|S+T| \geq |S| + |T| - 1$. This extension of the Cauchy–Davenport inequality is attributed to I. Chowla [3].

4. ACYCLICITY

Suppose that for each pair A, B of nonempty finite subsets of G satisfying $|A| = |B|$ and $0 \notin B$, there exists an acyclic matching $A \rightarrow B$. We then say that G possesses the *acyclic matching property*.

$\mathbb{Z}/7\mathbb{Z}$ is an example of a group that has the matching property but not the acyclic matching property (recall Remark 2.5). However, by combining an observation about torsion-free abelian groups with a construction due to Alon et al. [1], we arrive at the following result:

Theorem 4.1. *Let G be a torsion-free abelian group. Then G possesses the acyclic matching property.*

Proof. There exists a total ordering of the elements of G that is compatible with its group structure [7]. One way to see this is to embed G in some vector space V over the rationals, as follows: G , being the quotient of a direct sum of copies of \mathbb{Z} , can be embedded in a quotient D of a direct sum of copies of \mathbb{Q} . The quotient of D by its torsion subgroup is a vector space V over \mathbb{Q} . Since the restriction to G of the natural map $D \rightarrow V$ is injective, we have the required embedding. Now observe that V can be made into a totally ordered abelian group by applying the well-ordering principle to some basis.

So we may assume that G comes to us as a totally ordered abelian group. Also, take G to be nontrivial, since $G = \{0\}$ has the acyclic matching property.

Now let A, B be nonempty finite subsets of G satisfying $|A| = |B|$ and $0 \notin B$. Partition B into two sets: $B^+ = \{b \in B \mid b > 0\}$ and $B^- = B \setminus B^+$. Let A_l consist of the $|B^+|$ largest elements of A and let $A_s = A \setminus A_l$. We will construct an acyclic matching $\pi : A \rightarrow B$ that maps A_s onto B^- and A_l onto B^+ .

If A_l is nonempty, index its elements as follows: $a_1 < \dots < a_{|A_l|}$. Define $\pi(a_1)$ to be the smallest element b of B^+ such that $a + b \notin A$. Such an element exists because there are only $|A_l| - 1$ elements of A greater than a_1 whereas every one of the $|A_l|$ elements $a_1 + b$, for $b \in B^+$, is greater than a_1 .

Suppose $\pi(a_1), \dots, \pi(a_k)$ have been defined for $k < |A_l|$ so that for each $i \leq k$, $\pi(a_i)$ is the smallest element b of $B^+ \setminus \{\pi(a_1), \dots, \pi(a_{i-1})\}$ such that $a_i + b \notin A$. There are only $|A_l| - k - 1$ elements of A greater than a_{k+1} whereas every one of the $|A_l| - k$ elements $a_{k+1} + b$, for $b \in B^+ \setminus \{\pi(a_1), \dots, \pi(a_k)\}$, is greater than a_{k+1} . Hence, we may define $\pi(a_{k+1})$ to be the smallest element b of $B^+ \setminus \{\pi(a_1), \dots, \pi(a_k)\}$ such that $a_{k+1} + b \notin A$. This procedure defines π on all of A_l . Define π from A_s to B^- in the same way, using the opposite order on G .

We claim that π is acyclic. Let $\tau : A \rightarrow B$ be a matching satisfying $m_\tau = m_\pi$. Then $\tau(A_s) = B^-$ and $\tau(A_l) = B^+$. If A_l is empty, this is obvious. Suppose A_l is nonempty, and observe $\sum_{g > a_1} m_\tau(g) = \sum_{g > a_1} m_\pi(g) = |A_l|$. Hence, there exists a subset A' of A of size $|A_l|$ such that

$$\sum_{a \in A'} a + \tau(a) = \sum_{g > a_1} m_\tau(g) \cdot g = \sum_{g > a_1} m_\pi(g) \cdot g = \sum_{a \in A_l} a + \pi(a).$$

Since $\pi(A_l) = B^+$, this forces $A' = A_l$ and $\tau(A_l) = B^+$.

Assume for contradiction that $\tau \neq \pi$ on A_l (the case $\tau \neq \pi$ on A_s is handled similarly). Let g be the smallest element of G such that

$$\{a \in A_l \mid a + \tau(a) = g\} \neq \{a \in A_l \mid a + \pi(a) = g\}.$$

Let a be the smallest element in $\{a \in A_l \mid a + \tau(a) = g\} \setminus \{a \in A_l \mid a + \pi(a) = g\}$. If $\pi(a) < \tau(a)$, then the element $g' = a + \pi(a) < a + \tau(a)$ contradicts our choice of g . Hence $\pi(a) > \tau(a)$. By our construction of π , there exists $a' \in A_l$ such that $a' < a$ and $\pi(a') = \tau(a)$. But then $a' + \pi(a') = a' + \tau(a) < a + \tau(a)$, again contradicting our choice of g . The proof is complete. \square

Remark 4.2. When $A = B$, Theorem 4.1 can be restated as follows: Let a_1, \dots, a_n be distinct nonzero elements of a torsion-free abelian group G . Then at least one of the $n!$ diagonals of the matrix $\{a_i + a_j\}$ contains no a_i and is distinct as a multiset from the other diagonals.

Remark 4.3. Interest in acyclic matchings arose from consideration of the problem of determining the sets of monomials of a generic homogeneous polynomial that are removable through a linear change in variables. For details, see [6].

Remark 4.4. The basic matching problem considered in this paper can be reformulated for a non-abelian group G in some obvious ways. Further investigation along those lines could prove to be worthwhile.

5. ACKNOWLEDGMENT

The author is indebted to C. Kenneth Fan for his many helpful suggestions, including one that made apparent the relevance of the Cauchy–Davenport inequality to Theorem 3.1.

REFERENCES

- [1] N. Alon, C.K. Fan, D. Kleitman and J. Losonczy, Acyclic matchings, *Adv. Math.* **122** (1996), 234–236.
- [2] A. Cauchy, Recherches sur les nombres, *J. Ecole polytechn.* **9** (1813), 99–116.
- [3] I. Chowla, A theorem on the addition of residue classes: Application to the number $\Gamma(k)$ in Waring’s problem, *Proc. Indian Acad. Sci.* **2** (1935), 242–243.
- [4] H. Davenport, On the addition of residue classes, *J. London Math. Soc.* **10** (1935), 30–32.
- [5] H. Davenport, A historical note, *J. London Math. Soc.* **22** (1947), 100–101.
- [6] C.K. Fan and J. Losonczy, Matchings and canonical forms for symmetric tensors, *Adv. Math.* **117** (1996), 228–238.
- [7] F.W. Levi, Ordered groups, *Proc. Indian Acad. Sci.* **16** (1942), 256–263.
- [8] H.B. Mann, “Addition Theorems: The Addition Theorems of Group Theory and Number Theory,” Interscience Publishers, New York, London, Sydney, 1965.
- [9] M.B. Nathanson, “Additive Number Theory: Inverse Problems and the Geometry of Sumsets,” Springer-Verlag, New York, Berlin, Heidelberg, 1996.

MATHEMATICS DEPARTMENT, CITY UNIVERSITY OF NEW YORK, GRADUATE SCHOOL AND UNIVERSITY CENTER, NEW YORK, NY 10036

Article appeared in: *Advances in Applied Mathematics* **20** (1998), 385–391.