MTA SZTAKI Közlemények 34/1986 pp.175-184

LATTICE POINTS IN DIFFERENCE SETS

B. UHRIN

MTA SZTAKI

1. Let A be any Lebesgue-measurable set in R^n. By the difference set of A we mean the algebraic difference of A with itself. We shall denote this set by DA, i.e. $DA := A - A$. DA is clearly symmetric (about the origin), i.e. $DA = -DA$. The most familiar example for a difference set is any symmetric (about Θ) convex set K, because $K = D(\frac{1}{2} K)$. Denote by $\Lambda \subset R^n$ the set of points having integer coordinates (lattice points). The quotient space R^n/Λ is usually identified with the set $P := \{x \in R^n : 0 \leq x_i < 1, \quad i = 1,\dots,n\}$. The cardinality of the finite set $S \subset R^n$ will be denoted by $|S|$.
The present note studies the question: what is the connection between $|DA \cap \Lambda|$ and the volume (L-measure) $V(A)$ of A? It is intuitively clear that if $V(A)$ is too small then we cannot in general expect that DA will contain non-zero lattice points. For example the open unit hypercube $C := \{x \in R^n: \ |x_i| < 1, \quad i = 1,\dots,n\}$ has the volume $V(C)=2^n$, but the only lattice point in C is the origin Θ. However if we increase this set a little, i.e. take the set $C' := \{x: |x_i| < 1+\varepsilon, \quad i=1,\dots,n\}$, where $\varepsilon > 0$ is arbitrarily small, then $V(C') > 2^n$ and $|C' \cap \Lambda| = 3^n$.
The latter example reflects a more general rule: if for any symmetric (about Θ) convex set K we have $V(K) > 2^n$ then $|K \cap \Lambda| > 1$. (This is the well known Minkowski's convex body theorem, see [1].) Taking into account that $V(K)/2^n = V(\frac{1}{2} K)$, we can formulate this statement in terms of $D(\frac{1}{2} K)$:
$V(\frac{1}{2}K) > 1 \Rightarrow |D(\frac{1}{2} K) \cap \Omega| > 1$.

AMS Classification Numbers (1980): 10E05, 10E30.

This result proved to be true for any measurable set A: if $V(A) > 1$ then $|DA \cap \Lambda| > 1$. (This is the generalization of Minkowski's theorem due to Blichfeldt, see [1]).
On the other hand, let us look at the set S on Figure 1.

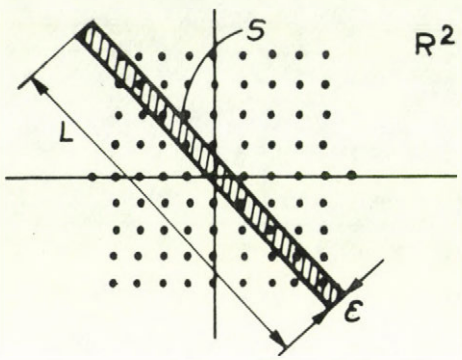

Figure 1

It is symmetric and convex, its volume is εL, but it contains $\sim L/\sqrt{2}$ lattice points. So we have a set of "almost zero volume" containing "almost infinitely many lattice points".
The basic aim of this note is to give a rule which sharpens the Blichfeldt's result and which works also in the above case of "thin sets of small volume containing many lattice points". The second aim is to present a new method of proof which seems to be at most natural and simple when compared with known ones.

2. The basic tool in our investigations will be the so called lexicographic ordering of points in R^n, denoted by "$\succ$". It is defined as follows: $x \succ \Theta$ if and only if either $x_1 > 0$ or $x_1 = x_2 = \ldots = x_i = 0$ and $x_{i+1} > 0$ for some $1 \leq i < n$.
Of course, $x \succ y$ means $x-y \succ \Theta$. This is a total (linear) ordering in R^n consistent with the addition of vectors.
Let $H \subset R^n$, be any finite set containing the zero vector Θ and symmetric about Θ (i.e. $H = -H$). If we want to list all elements of H, we can proceed in the following way:

First take Θ. Secondly, take $h_1 \in H$ that is the first positive (in the ordering $\succ$) element of H (i.e. $h_1 \succ \Theta$ and there is no $h \in H$ such that $h_1 \succ h \succ \Theta$). It is clear that $-h_1 \in H$ and $-h_1$ is the first negative element of H ($-h_1 \prec \Theta$ and there is no $h \in H$ s.t. $-h_1 \prec h \prec \Theta$). Take the second positive element of H, h_2, (i.e. $h_2 \succ h_1$ and there is no $h \in H$ s.t. $h_2 \succ h \succ h_1$). Again $-h_2$ is the second negative element of H. And so on. In this way we list all elements of H and we get

$$H = \{-h_q \prec -h_{q-1} \prec \ldots -h_1 \prec h_o = \Theta \prec h_1 \prec h_2 \prec \ldots \prec h_q\}.$$

At the same time we have just also proved that $|H|$ is an odd number. Now, let $A \subset R^n$ be an arbitrary measurable and bounded set. Applying the previous remark, we have for some $p \geq 1$

$$(1) \quad DA \cap \Lambda = \{-b_{p-1} \prec -b_{p-2} \prec \ldots \prec -b_1 \prec \Theta \prec b_1 \prec b_2 \prec \ldots \prec b_{p-1}\},$$

showing that

$$(2) \qquad |DA \cap \Lambda| = 2p-1.$$

The relation (2) implies that

$$(3) \qquad |A \cap \Lambda| \leq p.$$

Indeed, assume that $q = |A \cap \Lambda| > p$. Writing $A \cap \Lambda$ in the order $\succ$, we have $A \cap \Lambda = \{a_1 \prec a_2 \prec \ldots \prec a_q\}$. The elements $a_1 - a_q \prec a_1 - a_{q-1} \prec \ldots \prec a_1 - a_2 \prec \Theta \prec a_2 - a_1 \prec a_3 - a_1 \prec \ldots \prec a_q - a_1$ are mutually different and all belong to $DA \cap \Lambda$. This implies that $|DA \cap \Lambda| \geq 2q-1 > 2p-1$ that contradicts to (2). In general $A \cap \Lambda$ may be empty (hence $|A \cap \Lambda| = 0$) but (2) may hold with some $p > 1$. The second "extreme" case of (3) is when $|A \cap \Lambda| = p$. This implies quite strict conditions on the structure of $A \cap \Lambda$, namely we have

Proposition 1. Assume (2) holds and $|A \cap \Lambda| = p$. Then $A \cap \Lambda = \{a, a+d, a+2d, \ldots, a+(p-1)d\}$ for some $a \in \Lambda$ and $d > 0$ (i.e. $A \cap \Lambda$ is an arithmetic progression in the lexicographic ordering). □

The proposition will be a simple consequence of the following.

Lemma. Let $S, H \subset R^n$ be two finite non-empty sets. Let $S+H$ be their algebraic sum. Then

$$|S + H| \geq |S| + |H| - 1 \tag{5}$$

and equality is in (5) if and only if S and H are of the following form: $S = \{s, s+d, \ldots, s+(r-1)d\}$, $H = \{h, h+d, \ldots, h+(q-1)d\}$, where $d > 0$, $r = |S|$, $q = |H|$. □

Proof. Write S and H in the order $\succ$, say, $S = \{s_0 \prec s_1 \prec \ldots \prec s_{r-1}\}$, $H = \{h_0 \prec h_1 \prec \ldots \prec h_{q-1}\}$. Now we have

$$s_0+h_0 \prec s_0+h_1 \ldots \prec s_0+h_{q-1} \prec s_1+h_{q-1} \prec \ldots \prec s_{r-1}+h_{q-1}, \tag{6}$$

which proves (5).

The "if" part of the equality statement is clear. As to the "only if" part, denote $s_{ij} := s_i + h_j$ and $L_j := \{s_{00}, s_{01}, \ldots, s_{0j}, s_{1j}, s_{2j}, \ldots, s_{r-1,j}, s_{r-1,j+1}, \ldots, s_{r-1,q-1}\}$, $j = 0,1,\ldots,q-1$. Each L_j consists of lexicographically increasing sequence of elements, begins with s_{00} and ends with $s_{r-1,q-1}$. This implies, using the assumption $|S + H| = r + q - 1$, that each L_j represent the whole set $S + H$. This further implies that the k-th elements of any two L_j-s are equal, $k = 1,2,\ldots,r+q-1$. So we have for L_{j-1}, L_j and L_{j+1}: $s_i + h_{j-1} = s_{i-1} + h_j$, $s_{i+1} + h_{j-1} = s_i + h_j$, $s_{i+1} + h_j = s_i + h_{j+1}$. This implies: $d = s_i - s_{i-1} = s_{i+1} - s_i = h_j - h_{j-1} = h_{j+1} - h_j$.

Here i and j were arbitrary, so the lemma is proved. ■

Proof of the proposition: It is clear that

$$(6) \qquad D\mathrm{A} \cap \Lambda \supseteq D(\mathrm{A} \cap \Lambda).$$

Using (5) with $S := A \cap \Lambda$, $H := -(A \cap \Lambda)$, we have

$$(7) \qquad |D\mathrm{A} \cap \Lambda| \geq |D(\mathrm{A} \cap \Lambda)| \geq 2p - 1,$$

hence

$$(8) \qquad |D(\mathrm{A} \cap \Lambda)| = 2\,|\mathrm{A} \cap \Lambda| - 1.$$

The lemma now implies the result. ∎

The relation (2) implies a more general inequality, containing (3) as a special case. Namely, it is cleat that $D\mathrm{A}$ is invariant under the translations of A, i.e. $D(\mathrm{A}-x) = D\mathrm{A}$ for all $x \in R^n$. So (2) implies

$$(9) \qquad |D\mathrm{A} \cap \Lambda| = |D(\mathrm{A}-x) \cap \Lambda| = 2p - 1,$$

hence all results proved above hold for $A-x$ instead of A, say:

$$(10) \qquad |(A - x) \cap \Lambda| \leq p.$$

The function $|(A-x) \cap \Lambda|$ (of x) is periodic modΛ, i.e. $|(A-x+u) \cap \Lambda| = |(A-x) \cap \Lambda|$, $\forall x$, $\forall u$, hence when dealing with it we can restrict ourselves to the set P (a basic cell of Λ). (9) and (10) give

Proposition 2. For any set $A \subset R^n$ we have

$$(11) \qquad |D\mathrm{A} \cap \Lambda| \geq 2. \max_{x \in P} |(A-x) \cap \Lambda| - 1. \qquad \square$$

3. Let us study now the volume (L-measure) $V(A)$ of a L-measurable bounded set $A \subset R^n$. Using Λ, we get two decompositions of A:

$$A = \bigcup_{u \in \Lambda} ((P+u) \cap A) \quad , \tag{12}$$

$$A = \bigcup_{x \in P} (A \cap (\Lambda+x)) \quad . \tag{13}$$

In both decompositions the sets in the union are mutually disjoint. In (12) only finite number of sets are non-empty, hence

$$V(A) = \sum_{u \in \Lambda} V((P+u) \cap A) \tag{14}$$

(where the sum is finite).

In (13) each $A \cap (\Lambda+x)$ is finite, so we have to collect many of them to get sets of positive measure. This can be done, say, in such a way that we put together the sets $A \cap (\Lambda+x)$ having the same cardinality.
For this denote

$$A_i := \{x \in P : |A \cap (\Lambda+x)| = i\}, \quad i=0,1,2,\ldots \quad . \tag{15}$$

For $x \in A_i$, $i > 0$, the set $A \cap (\Lambda+x)$ is of the form

$$\{a_1(x) = u_1(x) + x,\ a_2(x) = u_2(x)+x, \ldots, a_i(x) = u_i(x)+x\}. \tag{16}$$

Let us partition A_i further according to the rule: $x,y \in A_i$ belong to the same set if $u_j(x) = u_j(y)$ for all $j=1,2,\ldots,i$. This will give a finite partition of A_i, say A_{ik}, $k = 1,2,\ldots,N(i)$.
Hence we can write

$$A = \bigcup_{i=1}^{\infty} \bigcup_{j=1}^{N(i)} \bigcup_{x \in A_{ij}} (A \cap (\Lambda + x)). \tag{17}$$

Clearly, there are $u_{1j}, u_{2j}, \ldots, u_{ij} \in \Lambda$ such that

$$\bigcup_{x \in A_{ij}} (A \cap (\Lambda + x)) = \bigcup_{k=1}^{i} (A_{ij} + u_{kj}). \tag{18}$$

Substituting (18) into (17) we get

$$V(A) = \sum_{i=1}^{\infty} i \cdot V(A_i). \tag{19}$$

The set

$$\varphi(A) := \bigcup_{i=1}^{\infty} A_i = \{x \in P: A \cap (\Lambda + x) \neq \emptyset\} \tag{20}$$

plays an important role in the algebraic theory of R^n. It is nothing else then the canonical map of A into the tours group R^n/Λ (after identifying R^n/Λ with P). This mapping is important also in our investigations. The quantity

$$V(\varphi(A)) = \sum_{i=1}^{\infty} V(A_i) \tag{21}$$

is the measure of the projection of A into R^n/Λ.

4. Now we put together the results of previous two sections to get main results of this note. It is clear that $|(A-x) \cap \Lambda| = |A \cap (\Lambda + x)|$ for all $x \in P$.

Proposition 3. For any bounded L-measurable set $A \subset R^n$ we have

$$|DA \cap \Lambda| \cdot V(\varphi(A)) \geq 2\, V(A) - V(\varphi(A)). \tag{22}$$

Proof. (19) and (21) shows that $V(A) = 0$ if and only if $V(\varphi(A)) = 0$. Let $V(A) > 0$. Inequality (11) implies that

$$|DA \cap \Lambda| \geq 2i - 1 \tag{23}$$

holds for all i such that $V(A_i) > 0$. Hence

$$|DA \cap \Lambda| \cdot V(A_i) \geq 2i\, V(A_i) - V(A_i). \tag{24}$$

Summing up both sides of (24) we get (22). ■

Proposition 4. Let A be as in Prop.3. If for some positive integer m we have $V(A)/V(\varphi(A)) > m$, then there are $u_i \in \Lambda$, $i = 1,\dots,m$, such that

$$\{-u_m \prec -u_{m-1} \prec \dots \prec -u_1 \prec \Theta \prec u_1 \prec u_2 \dots \prec u_m\} \subseteq DA \cap \Lambda. \tag{25}$$ □

Proof. Using (22) and (2) we see that $p-1 \geq m$, so (1) gives the result. □

This result is clearly sharper and more "exact" than that of Blichfeldt. Moreover, sets of the type seen on Fig.1 are succesfully treated by this rule. For such sets $V(A)$ may be very small, but $V(\varphi(A))$ is necessarily smaller (see (19) and (21)), so that their ratio may be quite big. For the investigation of this ratio the representations (19) and (21) are very useful.

5. In the course of our proofs we have used two structural properties of R^n only: it is an Abelian group having a total (linear) ordering consistent with the group operation. Hence all results are true in the same form for any topological Abelian group G and its discrete subgroup Λ, assuming that Λ can be totally ordered. (Of course we have also to assume that the quotient group G/Λ is compact.) In this case V means the Haar-measure in G.

The method sketched in this note can be succesfully developped to prove some estimations in geometry of numbers which are both more general and sharper than the known ones, see [2],[3].

REFERENCES

[1] C.G. Lekkerkerker, "Geometry of Numbers", Wolters-Noordhoff, Gronningen, North-Holland, Amsterdam, 1969.

[2] B. Uhrin, Some useful estimations in geometry of numbers, Period. Math. Hungar., 11 (2), (1980), 95-103.

[3] B. Uhrin, On a generalization of Minkowski's convex body theorem, J. of Number Theory, 13 (2), (1981), 192-209.

Differencia-halmazokban levő rácspontok

Uhrin Béla

Összefoglaló

A cikkben az $(A-A)\cap\Lambda$ halmaz számosságára vonatkozó alsó becslésektől van szó, ahol $A \subset R^n$ L-mérhető halmaz és Λ egy pontrács (diszkrét részcsoport) az R^n-ben. Az eredmények élesitik a klasszikus Minkowski-Rlichfeldt tételt a geometriai számelméletben.

Решеточные точки в разностных множествах

Б. Ухрин

Р е з ю м е

В статье изучаются нижние оценки для мощности множества $(A-A)\cap\Lambda$, где $A \subset R^n$ измеримое множество и Λ есть решетка /дискретная подгруппа/ в R^n. Результаты уточняют классический результат Минковского-Блихфелдта в геометрии чисел.