Article 14 INTEGERS 11A (2011)

Proceedings of Integers Conference 2009

ALGEBRAIC PROOF FOR THE GEOMETRIC STRUCTURE OF SUMSETS

Jaewoo Lee[1]

Department of Mathematics, Borough of Manhattan Community College, The City University of New York, New York, NY

jlee@bmcc.cuny.edu

Received: 1/26/10, Revised: 10/25/10, Accepted: 2/3/11, Published: 3/9/11

Abstract

We consider a finite set of lattice points and their convex hull. The author previously gave a geometric proof that the sumsets of these lattice points take over the central regions of dilated convex hulls, thus revealing an interesting connection between additive number theory and geometry. In this paper, we will see an algebraic proof of this fact when the convex hull of points is a simplex, exploring the connection between additive number theory and geometry further.

– Dedicated to Professor Mel Nathanson on the occasion of his 65th birthday

1. Background

Many interesting connections between number theory and geometry have been found over the years and we continue to find them even nowadays. To name a few, Athreya and Margulis [1] recently gave a random version of Minkowski's classical result on geometry of numbers. Nathanson [11, 12, 13] has found some interesting results in this area as well. In this paper, we will focus on how the sumset of a finite set of lattice points grows geometrically, which is our Theorem 7.

We use the following notation: For sets A, B of integers and for any integer t, we define the *sumset*

$$A + B = \{a + b : a \in A, b \in B\},$$

the *translation*

$$A + t = \{a + t : a \in A\},$$

[1]This work was supported in part by grants from the City University of New York Collaborative Incentive Research Grant Program and the PSC-CUNY Research Award Program.

and the *difference set*

$$A - B = \{a - b : a \in A, b \in B\}.$$

And for any nonnegative integer h, we define the *h-fold sumset* hA as follows:

$$hA = \{a_1 + a_2 + \cdots + a_h : a_1, a_2, \ldots, a_h \in A\}.$$

The *dilation* is

$$h * A = \{ha : a \in A\}.$$

The *convex hull* , $\text{conv}(x_1, x_2, \ldots, x_l)$, of $x_1, x_2, \ldots, x_l$ is

$$\Big\{x \in \mathbb{R}^n : \quad x = \lambda_1 x_1 + \lambda_2 x_2 + \cdots + \lambda_l x_l\,, \quad \lambda_i \geq 0 \text{ for all } i, \\ \text{and } \textstyle\sum_{i=1}^{l} \lambda_i = 1\Big\}\,.$$

A *polytope* is the convex hull of a finite set of points in some $\mathbb{R}^n$, or equivalently, a bounded set which is an intersection of finitely many closed halfspaces. In their book [2, page 26], Beck and Robins point out that this equivalence is highly non-trivial, both algorithmically and conceptually. You can find a proof of this in [14]. A *d-simplex* is the convex hull of any $d+1$ affinely independent points in some $\mathbb{R}^n$.

Note that the distance from a point $x \in \mathbb{R}^n$ to a hyperplane H where $x \notin H$, is given by the length of the perpendicular line segment from x to H. For, if not, say $y \in H$ is a point with $d(x, y) < d(x, x')$ where x' is the intersection of H and the perpendicular line segment. Then the points x, x', y form a right triangle whose hypotenuse is given by x and y, and the hypotenuse's length is shorter than that of the side given by x and x', which is impossible.

If two hyperplanes H_1, H_2 are parallel, their normal vectors are scalar multiples of each other, so we can take a same normal vector u and write $H_1 = \{x : (x, u) = \alpha_1\}$ and $H_2 = \{x : (x, u) = \alpha_2\}$ where $(\cdot\,,\cdot)$ indicates an inner product in $\mathbb{R}^n$. Take any $x \in H_1$. Then $d(x, H_2)$ is given by the length of the perpendicular line segment to H_2. To calculate the distance, note that $x + tu$ where $t \in \mathbb{R}$ gives the perpendicular ray from x to H_2 . If the ray meets H_2 when $t = t_2$, then $t_2 = (\alpha_2 - \alpha_1)/|u|^2$. Thus, $d(x, H_2) = |t_2 u| = (\alpha_2 - \alpha_1)/|u|$, which is independent of the choice of x. Therefore, when H_1 and H_2 are parallel, $d(H_1, H_2)$ is given by the length of any perpendicular line segment joining them.

For a fixed non-zero vector $u \in \mathbb{R}^n$ and a real number α, if the set $H = \{x : (x, u) = \alpha\}$ is a hyperplane, then the *half-spaces bounded by* H are $H^+ = \{x : (x, u) \geq \alpha\}$ and $H^- = \{x : (x, u) \leq \alpha\}$. H is called a *supporting hyperplane* of a polytope Δ if $\Delta \cap H \neq \emptyset$ and $\Delta \subseteq H^-$ or $\Delta \subseteq H^+$. And if H is a supporting hyperplane of Δ, then we call $F = \Delta \cap H$ a *face* of Δ. By convention, $\emptyset$ and Δ are called *improper faces* of Δ.

Let h be a positive integer and $\Delta = \mathrm{conv}(a_1, a_2, \ldots, a_m)$ where $a_i \in \mathbb{Z}^n$. Then the *dilation of* Δ, $h * \Delta$, is

$$\begin{aligned} h * \Delta &= \{hx : x \in \Delta\} \\ &= \{\sum \lambda_i a_i : \lambda_i \geq 0, \sum \lambda_i = h\} \\ &= \mathrm{conv}(ha_1, \ldots, ha_m) . \end{aligned}$$

We recall some elementary facts without proof. The details can be found in [3], [5], and [14].

Proposition 1. *We have the following:*

1. *Every polytope is a compact set.*
2. *Every polytope is the convex hull of its vertices.*
3. *If a polytope can be written as the convex hull of a finite point set S, then the finite set S contains all the vertices of the polytope, i.e., all the vertices of the polytope belong to S.*
4. *Let Δ be a polytope and V be the set of all vertices of Δ (called the vertex set). Let F be a face of Δ. Then the face F is again a polytope, with its vertex set $F \cap V$.*
5. *Every intersection of faces is a face of the polytope.*

Proposition 2. *Let Δ be a polytope in $\mathbb{R}^n$ of dimension n. Then the following are equivalent for $x \in \Delta$:*

1. *x is not contained in a proper face of Δ.*
2. *x can be represented in the form $x = \sum_{i=0}^{n} \lambda_i x_i$ for $n+1$ affinely independent points $x_0, x_1, \ldots, x_n \in \Delta$ with each $\lambda_i > 0$ and $\sum_{i=0}^{n} \lambda_i = 1$.*

If one of the conditions in Proposition 2 holds, then the point is called an *interior point* of Δ. It can be checked that this definition agrees with the usual definition of interior points in topology. The *boundary* of Δ, written $\partial(\Delta)$, is the union of all proper faces of Δ.

Assume that $\Delta \subseteq \mathbb{R}^n$ is an n-dimensional nonempty lattice polytope, and h is a positive integer. Then Ehrhart [4] showed that there is a polynomial $p(h)$, called the *Ehrhart polynomial*, such that

$$|(h * \Delta) \cap \mathbb{Z}^n| = p(h)$$

where

$$p(h) = \mathrm{Vol}(\Delta) h^n + \frac{\mathrm{Vol}(\partial(\Delta))}{2} h^{n-1} + \cdots + 1 .$$

Here, $\mathrm{Vol}(\partial(\Delta))$ is "the surface area of Δ normalized with respect to the sublattice on each face of Δ." For details, see [2].

If $\Delta = \mathrm{conv}(A)$ where A is a finite set of integral points in some $\mathbb{R}^n$, then $|(h*\Delta)\cap\mathbb{Z}^n| \geq |hA|$. Now we can consider the growth of hA instead. Nathanson [9] proved the following theorem.

Theorem 3. *Let $k \geq 2$ and let $A = \{a_1, \ldots, a_k\}$ be a finite set of integers such that*

$$0 = a_1 < a_2 < \cdots < a_k \text{ and } \gcd(a_2, \ldots, a_k) = 1.$$

Then there exists integers c and d and sets $C \subseteq [0, c-2]$ and $D \subseteq [0, d-2]$ such that

$$hA = C \cup [\, c, ha_k - d\,] \cup (ha_k - D)$$

for all sufficiently large h.

In particular, the growth of $|hA|$ is a linear function when A is a normalized subset of integers. When we have $A_1, A_2, \ldots, A_r$ and B as finite subsets of $\mathbb{N}_0$, normalized similarly as above, then Han, Kirfel, and Nathanson [6] showed that $|B+h_1A_1+\cdots+h_rA_r|$ is a multilinear function of $h_1, \ldots, h_r$ eventually. If $A_1, A_2, \ldots, A_r$ and B are finite subsets of an abelian semigroup which contains 0, then $|B+h_1A_1+\cdots+h_rA_r|$ is a polynomial of $h_1, \ldots, h_r$ for all sufficiently large $h_1, \ldots, h_r$. This was proven by Khovanskiĭ [7] when $r = 1$, and by Nathanson [10] for $r \geq 2$. And if A, B are finite subsets of an abelian group without elements of finite order, then Khovanskiĭ [7] computed the degree and the leading coefficient of the polynomial above.

In this paper, we will consider the growth of sumsets from geometric point of view.

2. Khovanskiĭ's Work

Before we talk about our main theorem, let us see what Khovanskiĭ did in his paper [7]. Let A be a finite subset of $\mathbb{Z}^n$, $A = \{a_1, \ldots, a_m\}$, with $|A| = m$ and $\Delta = \mathrm{conv}(A)$. Also assume that A generate $\mathbb{Z}^n$ as a group.

Lemma 4. *There exists a constant C with the following property: for all linear combination $\sum \lambda_i a_i$ of $a_i \in A$ with real coefficients λ_i such that $\sum \lambda_i a_i$ is an integral point, there exists a linear combination $\sum n_i a_i$ of a_i with integer coefficients such that $\sum n_i a_i = \sum \lambda_i a_i$, with $\sum |n_i - \lambda_i| < C$.*

Proof. Let $X = \{x : x \in \mathbb{Z}^n, x = \sum \lambda_i a_i,$ with $0 \leq \lambda_i \leq 1\}$, which is a finite set. Since A generate $\mathbb{Z}^n$, each $x \in X$ can be written as $x = \sum_{i=1}^m n_i(x) a_i$, where $n_i(x) \in \mathbb{Z}$. So for each $x \in X$, we fix one representation $\sum_{i=1}^m n_i(x) a_i$ with $n_i(x) \in \mathbb{Z}$. Let $q = \max_{x\in X} \sum_{i=1}^m |n_i(x)|$ and let $C = m + q$, a positive integer.

Then for any $z = \sum \lambda_i a_i \in \mathbb{Z}^n$, $x = z - \sum [\lambda_i] a_i \in X$. So $x = \sum_{i=1}^m n_i(x) a_i$ with $n_i(x) \in \mathbb{Z}$ and $z = \sum_{i=1}^m \big(n_i(x) + [\lambda_i]\big) a_i = \sum_{i=1}^m \lambda_i a_i$ with $\sum |n_i(x) + [\lambda_i] - \lambda_i| < \sum_{i=1}^m \big(|n_i(x)| + 1\big) \leq q + m = C$. □

Let h be a positive integer and assume $0 \in A$. Then

$$\Delta = \Big\{ \sum \lambda_i a_i : \lambda_i \geq 0, \sum \lambda_i \leq 1 \Big\}$$

and

$$h * \Delta = \Big\{ \sum \lambda_i a_i : \lambda_i \geq 0, \sum \lambda_i \leq h \Big\} .$$

Define

$$\Delta(h, C) = \Big\{ \sum \lambda_i a_i : \lambda_i \geq C \, , \sum \lambda_i \leq h - C \Big\}$$

with C as in Lemma 4.

Then, if $x = \sum \lambda_i a_i \in \Delta(h, C)$, let $\lambda_i = \alpha_i + C, \alpha_i \geq 0$. So

$$\begin{aligned} \Delta(h, C) &= \Big\{ \sum (\alpha_i + C) a_i : \ \alpha_i \geq 0 \, , \sum \alpha_i \leq h - C - mC \Big\} \\ &= C \sum a_i + \Big\{ \sum \alpha_i a_i : \ \alpha_i \geq 0 \, , \sum \alpha_i \leq h - C - mC \Big\} \\ &= C \sum a_i + (h - C - mC) * \Delta \, . \end{aligned}$$

Note $\Delta(h, C)$ is an empty set when $h < C + mC$, a single point $C \sum a_i$ when $h = C + mC$, and a dilation of Δ translated by an integral point when $h \geq C + mC + 1$.

If $x \in h * \Delta$, then $x = h(\sum \lambda_i a_i)$ where $\lambda_i \geq 0$, $\sum \lambda_i = 1$, so $x = \sum \lambda_i (h a_i) \in \operatorname{conv}(hA)$. Now, if $x \in \operatorname{conv}(hA)$, then

$$\begin{aligned} x &= \sum_i \lambda_i (a_i^1 + \cdots + a_i^h) \, , \ \lambda_i \geq 0 \, , \ \sum_i \lambda_i = 1 \\ &= h \sum_i \frac{\lambda_i}{h} (a_i^1 + \cdots + a_i^h) \\ &= h \sum_{j,k} \mu_{j,k} a_j^k \quad \text{where } \mu_{j,k} \geq 0, \ \sum_{j,k} \mu_{j,k} = \sum_i \frac{\lambda_i}{h} \cdot h = 1 \end{aligned}$$

by collecting terms for each a_j^k. So, $x \in h * \Delta$. Thus, $h * \Delta = \operatorname{conv}(hA)$. Also, $h * \Delta = \operatorname{conv}(h a_1, \ldots, h a_m)$.

Let $\mathbb{Z}^n(A)$ be the group generated by the differences of the elements of A .

Lemma 5. *Assume $\mathbb{Z}^n(A) = \mathbb{Z}^n$, and $0 \in A$. Then, every integral point in $\Delta(h, C)$ belongs to the sumset hA .*

Proof. Let z be an integral point in $\Delta(h, C)$. Then

$$z = \sum \lambda_i a_i, \quad \lambda_i \geq C \, , \sum \lambda_i \leq h - C \, .$$

By Lemma 4, $z = \sum n_i a_i\,,\ n_i \in \mathbb{Z}\,, \sum |n_i - \lambda_i| < C\,.$ If $n_i < 0$ for some i, then $|n_i - \lambda_i| > C$, so every n_i must be nonnegative. And $\sum n_i = \sum |n_i| = \sum |n_i - \lambda_i + \lambda_i| \le \sum |n_i - \lambda_i| + \sum |\lambda_i| < C + h - C = h\,.$ Thus $z = \sum n_i a_i\,,\ n_i \ge 0\,, \sum n_i < h\,.$ Since $0 \in A\,,$

$$hA = \Big\{ \sum n_i a_i : n_i \ge 0,\ \sum n_i \le h \Big\}\,,$$

and therefore $z \in hA\,.$ □

3. Main Theorem and Its Proof

Let K be the convex hull of $\{e_o, e_1, \dots, e_n\}$ in $\mathbb{R}^n$ where $e_0 = 0\,,$ and e_i for $i \ge 1$ is the ith standard basis in $\mathbb{R}^n\,.$ Then

$$\begin{aligned} h * K &= \Big\{ \sum_{i=0}^{n} \lambda_i e_i : \lambda_i \ge 0,\ \sum_{i=0}^{n} \lambda_i \le h \Big\} \\ &= \Big\{ \sum_{i=1}^{n} \lambda_i e_i : \lambda_i \ge 0,\ \sum_{i=1}^{n} \lambda_i \le h \Big\} \end{aligned}$$

and

$$\begin{aligned} K(h,C) &= \Big\{ \sum_{i=0}^{n} \lambda_i e_i : \lambda_i \ge C,\ \sum_{i=0}^{n} \lambda_i \le h - C \Big\} \\ &= \Big\{ \sum_{i=1}^{n} \lambda_i e_i : \lambda_i \ge C,\ \sum_{i=1}^{n} \lambda_i \le h - 2C \Big\}\,. \end{aligned}$$

Lemma 6. *For any positive integer $h\,,$ if a point in $h * K$ has the distance to $\partial(h * K)$ bigger than $2C$, then it belongs to $K(h,C)\,.$*

Proof. Let $z = \sum_{i=1}^{n} \lambda_i e_i\,,\ \lambda_i \ge 0, \sum \lambda_i \le h$ be such a point. Note we have $h * K = H_1^+ \cap \cdots \cap H_n^+ \cap H_{n+1}^+$ where hyperplanes $H_i = \{x_i = 0\}$ for $i = 1, \dots, n$ and the hyperplane $H_{n+1} = \{x \in \mathbb{R}^n : (x, \mathfrak{u}) = h\}$ where $\mathfrak{u}$ is the vector in $\mathbb{R}^n$ whose coordinates are all 1, $(\cdot\,,\cdot)$ indicates an inner product in $\mathbb{R}^n$, and H_i^+ denotes the closed half-space supported by the hyperplane H_i. So $h * K$ has its boundaries given by hyperplanes $H_1, \dots, H_n, H_{n+1}\,.$ Since $d(z, H_i) > 2C,\ \lambda_i > 2C$ for all $i = 1, \dots, n$. Now, let $H = \{x : (x, \mathfrak{u}) = h - 2C\}$, a hyperplane which is parallel to $H_{n+1}\,.$ Let $z_1 \in H$. Then, $z_1 + t\mathfrak{u},\ t \in \mathbb{R}$ is a ray starting from z_1 that is perpendicular to $H_{n+1}\,,$ and it will intersect H_{n+1} at, say, $t = t_2\,.$ Then $z_1 + t_2\mathfrak{u} \in H_{n+1}\,,$ so $(z_1 + t_2\mathfrak{u}, \mathfrak{u}) = h$, giving $t_2 = 2C/n\,.$ Thus, $d(H, H_{n+1}) = t_2|\mathfrak{u}| = 2C/\sqrt{n}\,.$ Now take any point x which lies between H and H_{n+1}. Then $d(x, H_{n+1})$ is given by the length of the line segment from x to H_{n+1} which is perpendicular to $H_{n+1}\,.$ If you extend this line segment so that it joins H and H_{n+1}, the length of this extended line segment, which is perpendicular to both H and H_{n+1} , gives $d(H, H_{n+1})$. Therefore, $d(x, H_{n+1}) < d(H, H_{n+1}) = 2C/\sqrt{n}$ for any point x which lies between H and H_{n+1}. Therefore, any point in $h * K$ whose distance to H_{n+1} is bigger than $2C/\sqrt{n}$ belongs to $H^- = \{x : (x, \mathfrak{u}) \leq h - 2C\}$. Therefore, $z \in H^-$, i.e., $\sum \lambda_i \leq h - 2C$. So $z \in K(h, C)$. □

Now we state our main theorem.

Theorem 7. *Suppose $\mathbb{Z}^n(A) = \mathbb{Z}^n$. Then, there exists a constant ρ with the following property: for any positive integer h, every integral point of $h * \Delta$ whose distance to $\partial(h * \Delta)$ is more than ρ belongs to the sumset hA.*

In general, hA is a subset of $(h * \Delta) \cap \mathbb{Z}^n$. Theorem 7 states that hA takes all of the central region in $h * \Delta$.

Without loss of generality, we may assume $0 \in A$ because: if not, by Proposition 1, all vertices of Δ belong to A. So take any $a \in A$ which is also a vertex of Δ, then take $\bar{\Delta} = \Delta - a$ so that $0 \in \bar{\Delta}$. Then $\bar{\Delta} = \operatorname{conv}(A - a)$ and $h * \bar{\Delta} = h * \Delta - ha = h * \operatorname{conv}(A - a)$. And, for any positive integer h, if $x \in (h * \Delta) \cap \mathbb{Z}^n$ with $d(x, \partial(h * \Delta)) > \rho$, then $x - ha \in h * \bar{\Delta}$, and $d(x - ha, \partial(h * \bar{\Delta})) > \rho$ since a translation does not change the distance. Thus $x - ha \in h(A - a) = hA - ha$ according to our theorem. So $x \in hA$, proving our claim. Therefore, we will assume $a_1 = 0$ from now on.

Using the ideas described in Section 2, Khovanskiĭ stated Theorem 7 in his paper [7], but his proof contained an error. However, we can modify his idea to obtain the following theorem for the simplex.

Theorem 8. *Suppose $\mathbb{Z}^n(A) = \mathbb{Z}^n$, and $A = \{a_1, a_2, \ldots, a_{n+1}\}$ are $n + 1$ affinely independent points. Then there exists a constant ρ with the following property: for any positive integer h, every integral point of $h * \Delta$ whose distance to $\partial(h * \Delta)$ is more than ρ belongs to the sumset hA.*

The affine hull $\operatorname{aff}(A)$ is an affine subspace, which is a translation of a linear subspace L, i.e., $\operatorname{aff}(A) = x + L$ for some $x \in \mathbb{R}^n$. So $A \subseteq x + L$. Therefore, if $\mathbb{Z}^n(A) = \mathbb{Z}^n$, then $\dim(\operatorname{aff}(A)) = \dim \Delta = n$.

Proof. Recall that we may assume $a_1 = 0$. Consider a linear mapping $\pi : \mathbb{R}^n \to \mathbb{R}^n$ where $\pi(e_i) = a_{i+1}$, i.e., $\pi(x) = Tx$ where T is the matrix whose ith column is given by the coordinates of a_{i+1} for $i = 1, \ldots, n$. Since $a_2 - a_1, \ldots, a_{n+1} - a_1$ are linearly independent, i.e., $a_2, \ldots, a_{n+1}$ are linearly independent, T is invertible so that π is injective. Also, $\pi(h * K) = h * \Delta$ and $\pi(K(h, C)) = \Delta(h, C)$. By Proposition 1, every proper face of $h * K$ is the convex hull of up to n vertices, and so is every proper face of $h * \Delta$.

Now, suppose $x \in h * \Delta$ belongs to a convex hull of up to n vertices. Recall that every vertex belongs to the set $\{ha_1, \ldots, ha_{n+1}\}$ by Proposition 1. Thus,

x belongs to the convex hull of a proper subset of $\{ha_1, \ldots, ha_{n+1}\}$. Take, for example, $x = \sum_{i=1}^{n} \lambda_i(ha_i)$, $\lambda_i \geq 0$, $\sum \lambda_i = 1$ (other cases are similar). Assume x is an interior point. Then by Proposition 2, x can be written as

$$x = \sum_{j=1}^{n+1} \gamma_j x_j \,, \qquad \text{where } \sum \gamma_j = 1,$$
$$x_j \in h * \Delta = \mathrm{conv}(ha_1, \ldots, ha_{n+1}),$$
$$x_j \text{ are affinely independent}$$
$$\text{and } \gamma_j > 0.$$

Then $x_j = \sum_{l=1}^{n+1} \alpha_{lj}(ha_l)$ with $\sum_{l=1}^{n+1} \alpha_{lj} = 1,\ \alpha_{lj} \geq 0$. So

$$\sum_{i=1}^{n} \lambda_i(ha_i) = \sum_{j=1}^{n+1} \sum_{l=1}^{n+1} \gamma_j \alpha_{lj}(ha_l) \tag{1}$$
$$\text{where } \sum_{j=1}^{n+1} \sum_{l=1}^{n+1} \gamma_j \alpha_{lj} = 1.$$

Since ha_i are affinely independent, the affine combinations of them are unique, so the coefficient of a_{n+1} in the right hand side of (1) must be 0. Therefore, $\sum_{j=1}^{n+1} \gamma_j \alpha_{(n+1)j} = 0$, but $\alpha_{lj} \geq 0$ and $\gamma_j > 0$. So $\alpha_{(n+1)j} = 0$ for all $j = 1, \ldots, n+1$. Thus $x_1, \ldots, x_{n+1} \in \mathrm{aff}(ha_1, \ldots, ha_n)$, which means there are $n+1$ affinely independent vectors in the affine hull $\mathrm{aff}(ha_1, \ldots, ha_n)$, whose dimension is $n-1$, giving us a contradiction. Therefore, $x \in \partial(h * \Delta)$. Similarly, if $x \in h * K$ belongs to a convex hull of up to n vertices, $x \in \partial(h * K)$. Thus we have just proved that

$$\partial(h * \Delta) = \big\{x \in h * \Delta : x \text{ belongs to a convex hull of up to } n \text{ vertices}\big\}$$

and

$$\partial(h * K) = \big\{x \in h * K : x \text{ belongs to a convex hull of up to } n \text{ vertices}\big\}.$$

Therefore, π maps $\partial(h * K)$ onto $\partial(h * \Delta)$.

Now, let $x \in h * \Delta$ be an integral point with $d(x, \partial(h * \Delta)) > 2C||\pi||$ where $||\pi||$ is the norm of π. Since π is injective, we have a unique point $\pi^{-1}(x)$. Then, for any $\bar{y} \in \partial(h * K)$, $\pi(\bar{y}) = y \in \partial(h * \Delta)$ and

$$|\pi^{-1}(x) - \bar{y}| \geq \frac{|x-y|}{||\pi||} > \frac{2C||\pi||}{||\pi||} = 2C.$$

Then, by Lemma 6, $\pi^{-1}(x) \in K(h, C)$. Therefore, $x \in \Delta(h, C)$. Thus, by Lemma 5, $x \in hA$. $\square$

Notice this proof is algebraic in nature. To prove Theorem 7 in its full strength, we had to use geometric arguments. For details, see [8]. In Section 1, we mentioned two equivalent definitions of a polytope (one is algebraic and the other is geometric). Each is used, in different ways, in our proofs for the geometric growth of sumsets.

Acknowledgment. The author thanks the referee for his/her helpful advice for improving this paper.

References

[1] J. Athreya and G. Margulis, *Logarithm laws for unipotent flows, I*, J. Mod. Dyn. **3** (2009), 359-378.

[2] M. Beck, and S. Robins, *Computing the Continuous Discretely*, Springer, 2007.

[3] A. Brøndsted, *An Introduction to Convex Polytopes*, Springer, 1983.

[4] E. Ehrhart, *Sur un problème de géométrie diophantienne linéaire II*, J. Reine Angew. Math. **227** (1967), 25-49.

[5] G. Ewald, *Combinatorial Convexity and Algebraic Geometry*, Springer, 1996.

[6] S. Han, C. Kirfel and M. B. Nathanson, *Linear forms in finite sets of integers*, Ramanujan J. **2** (1998), 271-281.

[7] A. G. Khovanskiĭ, *The Newton polytope, the Hilbert polynomial and sums of finite sets*(Russian), Funktsional. Anal. i Prilozhen. **26** (1992), no. 4, 57-63, 96; translation in Funct. Anal. Appl. **26** (1992), no.4, 276-281 (1993).

[8] J. Lee, *Geometric structure of sumsets*, preprint.

[9] M. B. Nathanson, *Sums of finite sets of integers*, Amer. Math. Monthly **79** (1972), 1010-1012.

[10] M. B. Nathanson, *Growth of sumsets in abelian semigroups*, Semigroup Forum **61** (2000), no. 1, 149-153.

[11] M. B. Nathanson, *Bi-Lipshitz equivalent metrics on groups, and a problem in additive number theory*, preprint.

[12] M. B. Nathanson, *An inverse problem in number theory and geometric group theory*, in: Additive Number Theory. Festschrift In Honor of the Sixtieth Birthday of Melvyn B. Nathanson, D. Chudnovsky and G. Chudnovsky (eds.), Springer, 2010, 249-258.

[13] M. B. Nathanson, *Phase transitions in infinitely generated groups, and related problems in additive number theory*, Number Theory. New York Seminar, *to appear.*

[14] G. M. Ziegler, *Lectures on Polytopes*, Springer, 1995