Publ. Math. Debrecen
79/3-4 (2011), 563–572
DOI: 10.5486/PMD.2011.5087

Geometric group theory and arithmetic diameter

By MELVYN B. NATHANSON (New York)

To K. Győry and A. Sárközy on their 70th birthdays and A. Pethő and J. Pintz on their 60th birthdays

Abstract. Let X be a group with identity e, let A be an infinite set of generators for X, and let (X, d_A) be the metric space with the word metric d_A induced by A. If the diameter of the space is infinite, then for every positive integer h there are infinitely many elements $x \in X$ with $d_A(e, x) = h$. It is proved that if $\mathcal{P}$ is a nonempty finite set of prime numbers and A is the set of positive integers whose prime factors all belong to $\mathcal{P}$, then the metric space $(\mathbf{Z}, d_A)$ has infinite diameter. Let $\lambda_A(h)$ denote the smallest positive integer x with $d_A(e, x) = h$. It is an open problem to compute $\lambda_A(h)$ and estimate its growth rate.

1. Word metrics on infinitely generated groups

There is a nice interaction between geometric group theory and additive number theory, and concepts from each have fruitful analogs in the other. Indeed, a large part of geometric group theory can be considered as a kind of "nonabelian additive number theory." We shall consider growth in groups with a fixed infinite set of generators. The group of integers, of course, is of unique interest to number theorists, and we describe some problems and results about additive bases of infinite order that arise in geometry.

Let $\mathbf{N}_0$ denote the nonnegative integers and $\mathbf{Z}$ the integers.

Mathematics Subject Classification: 05A17,11B05,11B13, 11P99, 20F65.
Key words and phrases: additive number theory, geometric group theory, arithmetic diameter, word metrics, sums of powers, exponential diophantine equations, geometric number theory.

Let X be a group, written multiplicatively, with identity e. For $A \subseteq X$, we define $A^{-1} = \{a^{-1} : a \in A\}$. A subset A of X is a *generating set* for X if every element of X can be written as a finite product of elements of A and their inverses. Equivalently, A generates X as a group if and only if $A \cup A^{-1}$ generates X as a semigroup. The *length* of an element $x \in X$ with respect to A is

$$\begin{aligned}\ell_A(x) &= \min\{k : x = a_1^{\varepsilon_1} a_2^{\varepsilon_2} \cdots a_k^{\varepsilon_k} : a_i \in A \text{ and } \varepsilon_i \in \{1, -1\} \text{ for } i = 1, 2, \ldots, k\} \\ &= \min\{k : x = a_1 a_2 \cdots a_k : a_i \in A \cup A^{-1} \text{ for } i = 1, 2, \ldots, k\}.\end{aligned}$$

Thus, in a group, $\ell_A(x)$ is the number of letters in the shortest word in the alphabet $A \cup A^{-1}$ that spells x.The length function of a group has the following properties:

(i) $\ell_A(x) \geq 0$ for all $x \in X$

(ii) $\ell_A(x) = 0$ if and only if $x = e$

(iii) For all $x, y \in X$,
$$\ell_A(xy) \leq \ell_A(x) + \ell_A(y)$$

(iv) For all $x \in X$,
$$\ell_A\left(x^{-1}\right) = \ell_A(x).$$

These properties of the length function imply that the function $d_A : X \times X \to \mathbf{N}_0$ defined by
$$d_A(x, y) = \ell_A\left(x^{-1}y\right)$$
is a distance function on the group X. We call d_A the *word metric* induced by A. Geometric properties of the metric space (X, d_A) are often related to combinatorial and additive number theoretic properties of the set A.

The definition of the length function also implies that, for all $x \in X$ and $a \in A \cup A^{-1}$,
$$\ell_A(x) - 1 \leq \ell_A(ax) \leq \ell_A(x) + 1 \tag{1}$$
$$\ell_A(x) - 1 \leq \ell_A(xa) \leq \ell_A(x) + 1 \tag{2}$$
and, if $\ell_A(x) = h$ and $x = a_1 a_2 \cdots a_h$ with $a_i \in A \cup A^{-1}$ for $i = 1, 2, \ldots, h$, then
$$\ell_A(a_{j+1} a_{j+2} \cdots a_k) = k - j \tag{3}$$
for all $0 \leq j < k \leq h$.

For every nonnegative integer h, the *sphere* of radius h with respect to A is the set
$$S_A(h) = \{x \in X_0 : \ell_A(x) = h\} \tag{4}$$

and the *closed ball* of radius h with respect to A is the set

$$\overline{B}_A(h) = \{x \in X_0 : \ell_A(x) \leq h\} = \bigcup_{h_1=0}^{h} S_A(h_1). \tag{5}$$

Most research in geometric group theory concerns finitely generated groups. In number theory, however, it is often important to study a group X with an infinite set A of generators. The generating set A is not necessarily minimal, and it is irrelevant whether or not the group can be finitely generated.

The following theorem is fundamental for the geometry of groups with an infinite number of generators. Recall that the *diameter* of a metric space (X, d) is

$$\operatorname{diam}(X) = \sup\{d(x, y) : x, y \in X\}.$$

Theorem 1 (Nathanson [5])**.** *Let X be a group and let A be an infinite generating set for X. If the sphere $S_A(h)$ is finite for some positive integer h, then $S_A(k) = \emptyset$ for all $k > h$. Equivalently, if $\operatorname{diam}(X) = \infty$, then $S_A(h)$ is an infinite set for every positive integer h.*

Proof. Let ℓ_A be the length function associated with the generating set A. Let h be a positive integer such that $S_A(h)$ is finite. The sphere $S_A(1) = \left(A \cup A^{-1}\right) \setminus \{e\}$ is infinite, and so $h \geq 2$. If $S_A(k) \neq \emptyset$ for some integer $k > h$, then there exist elements $a_1, \ldots, a_k \in A \cup A^{-1}$ such that

$$\ell_A(a_1 a_2 \cdots a_k) = k.$$

We define a function $f : A \to \{1, \ldots, k\}$ as follows. By (1) and (2), for every $a \in A$ we have

$$\ell_A(a a_1 a_2 \cdots a_k) \geq k - 1 \geq h$$

and so there is at least one integer $t \in \{1, \ldots, k\}$ such that

$$\ell_A(a a_1 a_2 \cdots a_t) = h.$$

Choose any t with $\ell_A(a a_1 a_2 \cdots a_t) = h$ and let $f(a) = t$. Because the set A is infinite and $A = \bigcup_{i=1}^{k} f^{-1}(i)$, it follows from the pigeonhole principle that $f^{-1}(t)$ is an infinite set for some $t \in \{1, \ldots, k\}$, and so there exist infinitely many elements $a \in A$ such that $a a_1 a_2 \cdots a_t$ has length h. If $a \neq a'$, then $a a_1 a_2 \cdots a_t \neq a' a_1 a_2 \cdots a_t$ and the finite set $S_A(h)$ must contain the infinite subset $\{a a_1 a_2 \cdots a_t : a \in f^{-1}(t)\}$, which is absurd. Thus, if $S_A(h)$ is finite for some $h \geq 2$, then $S_A(k) = \emptyset$ for all $k > h$. This completes the proof. □

2. Sum and difference sets for additive groups

If X is an additive abelian group with identity 0, then for every subset A of X and for every positive integer h, we define the h-fold *sum and difference set*

$$h^{\pm}A = \left\{ \sum_{i=1}^{h} \varepsilon_i a_i : \varepsilon_i \in \{1, -1\} \text{ and } a_i \in A \text{ for } i = 1, \ldots, h \right\}.$$

We define $0^{\pm}A = \{0\}$. If A generates the group X, then, in geometric group theory, the set

$$\overline{B}_A(h) = \bigcup_{h_1 \leq h} h_1^{\pm}A = h^{\pm}(A \cup \{0\})$$

is the closed ball of radius h in the metric space (X, d_A) with respect to the word metric d_A induced by the generating set A. The generating set A is called a *basis of order* h for X if $\overline{B}_A(h) = X$. The set A is a *basis of finite order* for X if $\overline{B}_A(h) = X$ for some positive integer h.

The sum and difference sets $h^{\pm}A$ are finite for all positive integers h if and only if the set A is finite. Moreover, if A is finite, then

$$|h^{\pm}A| \leq \binom{2|A| + h - 1}{h} \leq (2|A|)^h \tag{6}$$

and

$$\left|\overline{B}_A(h)\right| \leq \binom{2|A| + h}{h} \leq (2|A| + 1)^h \tag{7}$$

where $|A|$ denotes the cardinality of the set A.

Theorem 2. *Let A be a generating set for the group X. The set A is a basis of finite order for X if and only if the diameter of the metric space (X, d_A) is finite.*

Proof. The diameter of the metric space (X, d_A) is finite if and only if $\bar{B}_A(h) = X$ for some positive integer h. □

3. Arithmetic diameter

A nonempty subset A of the additive abelian group $\mathbf{Z}$ is a generating set for $\mathbf{Z}$ if and only if $\gcd(A) = 1$. The *arithmetic diameter* of a set A of relatively prime integers is the diameter of the metric space $(\mathbf{Z}, d_A)$. It is, in general, a difficult

problem to compute or to estimate the arithmetic diameter of a generating set, or even to describe the infinite generating sets whose arithmetic diameters are finite. In this section we prove that if $\mathcal{P}$ is a nonempty finite set of prime numbers and if A is the set of positive integers all of whose prime factors belong to A, then $\operatorname{diam}(\mathbf{Z}, d_A) = \infty$. We need the following beautiful result from analytic number theory.

Prachar's Theorem. *Let $\delta(n)$ denote the number of prime numbers p such that $p-1$ divides n. For every positive real number $c < (\log 2)/2$ and for every positive integer k_0, there exist infinitely many positive integers n such that*

$$\delta(n) > \exp\left(\frac{c \log n}{\log\log n}\right) + k_0.$$

Proof. See Prachar [7], or Adleman, Pomerance, and Rumely [1, Proposition 10]. □

Theorem 3. *Let $\mathcal{P}$ be a nonempty finite set of prime numbers and let A be the set of positive integers that are products of primes in $\mathcal{P}$, that is,*

$$A = \left\{ \prod_{p \in \mathcal{P}} p^{v_p} : v_p \in \mathbf{N}_0 \right\}.$$

Let d_A be the word metric induced by A on the group $\mathbf{Z}$. The diameter of the metric space $(\mathbf{Z}, d_A)$ is infinite. Equivalently, $h^{\pm}(A \cup \{0\}) \neq \mathbf{Z}$ for every positive integer h.

Proof. Let $\mathcal{Q}$ be a finite set of prime numbers that is disjoint from $\mathcal{P}$, and let

$$Q = \prod_{q \in \mathcal{Q}} q.$$

If $a \in A$ and $q \in \mathcal{Q}$, then $\gcd(a, q) = 1$ and

$$a^{q-1} \equiv 1 \pmod{q}.$$

Let n is an integer that is divisible by $q-1$ for all $q \in \mathcal{Q}$. Then

$$a^n \equiv 1 \pmod{q}$$

for all $q \in \mathcal{Q}$, and so

$$a^n \equiv 1 \pmod{Q}. \tag{8}$$

Let $\mathbf{Z}/Q\mathbf{Z}$ be the ring of congruence classes modulo Q. For every integer r, we denote the congruence class of r modulo Q by $\overline{r} = r + Q\mathbf{Z}$. For every set R of integers, we define

$$\overline{R} = \{\overline{r} : r \in R\} \subseteq \mathbf{Z}/Q\mathbf{Z}.$$

Consider the set of integers

$$R_Q = \left\{ \prod_{p \in \mathcal{P}} p^{j_p} : j_p \in \{0, 1, \ldots, n-1\} \right\}.$$

We have $R_Q \subseteq A$ and so $\overline{R_Q} \subseteq \overline{A}$.

Let $a = \prod_{p \in \mathcal{P}} p^{v_p} \in A$. By the division algorithm, for each prime $p \in \mathcal{P}$ there are integers w_p and j_p with $j_p \in \{0, 1, \ldots, n-1\}$ such that

$$v_p = w_p n + j_p.$$

Defining

$$a_1 = \prod_{p \in \mathcal{P}} p^{w_p} \in A$$

and

$$r = \prod_{p \in \mathcal{P}} p^{j_p} \in R_Q$$

we obtain

$$a = \prod_{p \in \mathcal{P}} p^{v_p} = \prod_{p \in \mathcal{P}} p^{w_p n + j_p} = \left(\prod_{p \in \mathcal{P}} p^{w_p} \right)^n \prod_{p \in \mathcal{P}} p^{j_p} = a_1^n r.$$

Congruence (8) implies that

$$a \equiv r \pmod{Q}$$

and so $\overline{a} = \overline{r} \in \overline{R_Q}$ for all $a \in A$, that is, $\overline{A} \subseteq \overline{R_Q}$, hence $\overline{A} = \overline{R_Q}$. Let

$$|\mathcal{P}| = k_0.$$

Then

$$|\overline{A}| = |\overline{R_Q}| \leq |R_Q| = n^{k_0}$$

and, by (7),

$$\left| h^{\pm} \left(\overline{R_Q} \cup \{\overline{0}\} \right) \right| \leq \left(2|\overline{R_Q}| + 1 \right)^h \leq \left(2n^{k_0} + 1 \right)^h < c_0 n^{k_0 h}$$

for $c_0 = 3^h$. If $\operatorname{diam}(\mathbf{Z}, d_A) = h$, then

$$h^{\pm}(A \cup \{0\}) = \mathbf{Z}$$

and so

$$\mathbf{Z}/Q\mathbf{Z} = \overline{h^{\pm}(A \cup \{0\})} = h^{\pm}\left(\overline{A} \cup \{\overline{0}\}\right) = h^{\pm}\left(\overline{R_Q} \cup \{\overline{0}\}\right)$$

and

$$Q = |\mathbf{Z}/Q\mathbf{Z}| = \left|h^{\pm}\left(\overline{R_Q} \cup \{\overline{0}\}\right)\right| < c_0 n^{k_0 h}.$$

Conversely, if we can construct a finite set $\mathcal{Q}$ of prime numbers that is disjoint from $\mathcal{P}$ and an integer n that is divisible by $q-1$ for every $q \in \mathcal{Q}$ such that $c_0 n^{k_0 h} < Q$, then $\operatorname{diam}(\mathbf{Z}, d_A) \neq h$. This is what we shall do.

Applying Prachar's theorem with $k_0 = |\mathcal{P}|$ and any positive number $c < (\log 2)/2$, we obtain arbitrarily large integers n with the property that there are at least

$$\delta(n) - k_0 > \exp\left(\frac{c \log n}{\log\log n}\right)$$

prime numbers q such that $q-1$ divides n and $q \notin \mathcal{P}$. For each such n, let $\mathcal{Q}_n$ be the set of these primes and let Q_n be the product of the primes in $\mathcal{Q}_n$. Then

$$Q_n \geq 2^{\delta(n)-k_0} > \exp\left(\log 2 \exp\left(\frac{c \log n}{\log\log n}\right)\right) > c_0 n^{k_0 h}$$

for n sufficiently large. This completes the proof. □

Theorem 4. *Let $\mathcal{P}$ be a nonempty finite set of prime numbers and let A be the set of positive integers that are products of primes in $\mathcal{P}$. Let h be a positive integer and let $S_A(h) = \{n \in \mathbf{Z} : \ell_A(n) = h\}$. Then $S_A(h)$ contains infinitely many integers for every positive integer h.*

Proof. This follows immediately from Theorem 1. □

Lemma 1. *Let A and A' be generating sets for $\mathbf{Z}$, with induced word metrics d_A and $d_{A'}$, respectively. If $A \subseteq A'$, then $d_A(x,y) \geq d_{A'}(x,y)$ for all $x, y \in \mathbf{Z}$. In particular, if the arithmetic diameter of the set A' is infinite, then the arithmetic diameter of the set A is infinite.*

Proof. This follows immediately from the definitions of word metric and diameter. □

Theorem 5. *Let $\{a_1, \ldots, a_k\}$ be a set of positive integers. The arithmetic diameter of the set $A = \bigcup_{i=1}^{k} \{a_i^j : j \in \mathbf{N}_0\}$ is infinite. Moreover, $\{n \in \mathbf{Z} : \ell_A(n) = h\}$ is infinite for every positive integer h.*

PROOF. Let $\mathcal{P}$ be the finite set consisting of all prime numbers p such that that p divides a_i for some $i = 1, \ldots, k$. Let A' be the set of positive integers all of whose prime factors belong to $\mathcal{P}$. Then $A \subseteq A'$. The set A' has infinite arithmetic diameter by Theorem 3, and so A has infinite arithmetic diameter by Lemma 1. The sphere $S_A(h) = \{n \in \mathbf{Z} : \ell_A(n) = h\}$ is infinite for every positive integer h by Theorem 4. This completes the proof. □

4. Open problems

The following result is a special case of Theorem 5.

Theorem 6. *For every positive integer h there are infinitely many positive integers N such that, for some nonnegative integers j and k with $h = j + k$, the exponential diophantine equation*

$$N = \pm 2^{v_1} \pm 2^{v_2} \pm \cdots \pm 2^{v_j} \pm 3^{w_1} \pm 3^{w_2} \cdots \pm 3^{w_k}$$

has a solution in nonnegative integers $v_1, \ldots, v_j, w_1, \ldots, w_k$, but the corresponding equations with h replaced by any positive integer $h' < h$ have no solution.

PROOF. Apply Theorem 5 to the set $\{2, 3\}$. □

Problem 1. *Theorem 6 implies that for every positive integer h there is a smallest number $N = \lambda_{2,3}(h)$ that can be written as the sum or difference of exactly h but no fewer powers of 2 and 3. For example, $\lambda_{2,3}(1) = 1$, $\lambda_{2,3}(2) = 5$, and $\lambda_{2,3}(3) = 21$. Satyanand Singh proved that $\lambda_{2,3}(4) = 150$. It is difficult to compute the function $\lambda_{2,3}(h)$, and it is an open problem to determine its rate of growth.*

Problem 2. *Let $\mathcal{P}$ be a nonempty finite set of prime numbers, and let A be the set of positive integers that are products of powers of primes in $\mathcal{P}$. By Theorem 3, for every positive integer h there are infinitely many positive integers of length h. Let $\lambda_{\mathcal{P}}(h)$ denote the smallest positive integer of length h. Determine the properties of this function. Estimate its growth rate.*

Problem 3. *Let $(a_i)_{i=1}^{\infty}$ be a strictly increasing sequence of positive integers, and let*

$$A = \bigcup_{i=1}^{\infty} \{a_i^j : j = i, i + 1.i + 2, \ldots\}.$$

Is A a basis of finite order for $\mathbf{Z}$? The condition $j \geq i$ is used to avoid Waring's problem.

Problem 4. *Let a and b be integers with $a \geq 2$ and $b \geq 2$, and let $(\mathbf{Z}, d_a)$ and $(\mathbf{Z}, d_b)$ be the metric spaces with the word metrics induced by the generating sets $\{a^i : i \in \mathbf{N}_0\}$ and $\{b^i : i \in \mathbf{N}_0\}$, respectively.* Nathanson [4] *proved that the word metrics d_a and d_b are bi-Lipschitz equivalent if and only if there exist positive integers m and n such that $a^m = b^n$. It is not know, however, under what conditions the metric spaces $(\mathbf{Z}, d_a)$ and $(\mathbf{Z}, d_b)$ are bi-Lipschitz equivalent. It is a problem of Richard E. Schwartz in metric geometry to determine if the metric spaces $(\mathbf{Z}, d_a)$ and $(\mathbf{Z}, d_b)$ are quasi-isometric. This is unknown even in the case $a = 2$ and $b = 3$.*

Problem 5. *Let A and B be infinite generating sets for $\mathbf{Z}$. Determine necessary and sufficient conditions for the metric spaces $(\mathbf{Z}, d_A)$ and $(\mathbf{Z}, d_B)$ to be quasi-isometric.*

5. Notes

Theorem 1 appears in Nathanson [5]. Hannah Alpert informed me that essentially the same result, but written in the language of graph theory, was proved by Wesley Pegden [6].

L. Hajdu and R. Tijdeman [2] have obtained a nontrivial upper bound for the function $\lambda_{2,3}(h)$. They observed that Theorem 3 was first proved by Jarden and Narkiewicz [3] in the language of algebraic number theory.

It is useful to be polylingual in mathematics.

Theorem 6 was proved by Gautam Chinta (personal communication), and the elementary proof of Theorem 3 in this paper is based on Chinta's method.

References

[1] L. M. Adleman, C. Pomerance and R. S. Rumely, On distinguishing prime numbers from composite numbers, *Ann. of Math.* (2)**117**, no. 1 (1983), 173–206.

[2] L. Hajdu and R. Tijdeman, Representing integers as linear combinations of powers, *Publ. Math. Debrecen* **79** (2011), 461–468.

[3] M. Jarden and W. Narkiewicz, On sums of units, *Monatsh. Math.* **150** (2007), 327–332.

[4] M. B. Nathanson, Bi-Lipschitz equivalent metrics on groups, and a problem in additive number theory, *Port. Math.* **68** (2011), 191–203.

[5] M. B. Nathanson, Phase transitions in infinitely generated groups, and related problems in additive number theory, *Integers* **11 A** (2011), 1–14, Article 17.

[6] W. Pegden, Distance sequences in locally infinite vertex-transitive digraphs, *Combinatorica* **26** (2006), 577–585.

[7] K. Prachar, Über die Anzahl der Teiler einer natürlichen Zahl, welche die Form $p-1$ haben, *Monatsh. Math.* **59** (1955), 91–97.

MELVYN B. NATHANSON
LEHMAN COLLEGE (CUNY)
BRONX, NY 10468
AND CUNY GRADUATE CENTER
NEW YORK, NY 10016
USA

E-mail: melvyn.nathanson@lehman.cuny.edu

(Received January 5, 2011; revised September 21, 2011)