Discrete Comput Geom (2008) 39: 59–66
DOI 10.1007/s00454-008-9059-9

Siegel's Lemma and Sum-Distinct Sets

Iskander Aliev

Received: 13 October 2005

Abstract Let $L(\mathbf{x}) = a_1x_1 + a_2x_2 + \cdots + a_nx_n$, $n \geq 2$, be a linear form with integer coefficients $a_1, a_2, \ldots, a_n$ which are not all zero. A basic problem is to determine nonzero integer vectors $\mathbf{x}$ such that $L(\mathbf{x}) = 0$, and the maximum norm $\|\mathbf{x}\|$ is relatively small compared with the size of the coefficients $a_1, a_2, \ldots, a_n$. The main result of this paper asserts that there exist linearly independent vectors $\mathbf{x}_1, \ldots, \mathbf{x}_{n-1} \in \mathbb{Z}^n$ such that $L(\mathbf{x}_i) = 0$, $i = 1, \ldots, n-1$, and

$$\|\mathbf{x}_1\| \cdots \|\mathbf{x}_{n-1}\| < \frac{\|\mathbf{a}\|}{\sigma_n},$$

where $\mathbf{a} = (a_1, a_2, \ldots, a_n)$ and

$$\sigma_n = \frac{2}{\pi} \int_0^\infty \left(\frac{\sin t}{t}\right)^n dt.$$

This result also implies a new lower bound on the greatest element of a sum-distinct set of positive integers (Erdös–Moser problem). The main tools are the Minkowski theorem on successive minima and the Busemann theorem from convex geometry.

1 Introduction

Let $\mathbf{a} = (a_1, \ldots, a_n)$, $n \geq 2$, be a nonzero integral vector. Consider the linear form $L(\mathbf{x}) = a_1x_1 + a_2x_2 + \cdots + a_nx_n$. Siegel's lemma with respect to the maximum norm

The work was partially supported by FWF Austrian Science Fund, Project M821-N12.

I. Aliev (✉)
School of Mathematics, University of Edinburgh, James Clerk Maxwell Building, King's Buildings, Mayfield Road, Edinburgh EH9 3JZ, Scotland
e-mail: I.Aliev@ed.ac.uk

$\|\cdot\|$ asks for an optimal constant $c_n > 0$ such that the equation

$$L(\mathbf{x}) = 0$$

has an integral solution $\mathbf{x} = (x_1, \ldots, x_n)$ with

$$0 < \|\mathbf{x}\|^{n-1} \le c_n \|\mathbf{a}\|. \tag{1}$$

The only known exact values of c_n are $c_2 = 1$, $c_3 = \frac{4}{3}$ and $c_4 = \frac{27}{19}$ (see [1] and [15]). Note that for $n = 3, 4$ the equality in (1) is not attained. Schinzel [15] showed that, for $n \ge 3$,

$$c_n = \sup \Delta\big(\mathcal{H}^{n-1}_{\alpha_1,\ldots,\alpha_{n-3}}\big)^{-1} \ge 1,$$

where $\Delta(\cdot)$ denotes the critical determinant, $\mathcal{H}^{n-1}_{\alpha_1,\ldots,\alpha_{n-3}}$ is a generalized hexagon in $\mathbb{R}^{n-1}$ given by

$$|x_i| \le 1, \quad i = 1, \ldots, n-1, \quad \left|\sum_{i=1}^{n-3} \alpha_i x_i + x_{n-2} + x_{n-1}\right| \le 1,$$

and α_i range over all rational numbers in the interval $(0, 1]$. The values of c_n for $n \le 4$ indicate that, most likely, $c_n = \Delta(\mathcal{H}^{n-1}_{1,\ldots,1})^{-1}$. However, a proof of this conjecture does not seem within reach at present. The best known upper bound

$$c_n \le \sqrt{n} \tag{2}$$

follows from the classical result of Bombieri and Vaaler [3, Theorem 1].

In this paper we estimate c_n via values of the sinc integrals

$$\sigma_n = \frac{2}{\pi} \int_0^\infty \left(\frac{\sin t}{t}\right)^n dt.$$

The main result is as follows:

Theorem *For any nonzero vector* $\mathbf{a} \in \mathbb{Z}^n$, $n \ge 5$, *there exist linearly independent vectors* $\mathbf{x}_1, \ldots, \mathbf{x}_{n-1} \in \mathbb{Z}^n$ *such that* $L(\mathbf{x}_i) = 0$, $i = 1, \ldots, n-1$, *and*

$$\|\mathbf{x}_1\| \cdots \|\mathbf{x}_{n-1}\| < \frac{\|\mathbf{a}\|}{\sigma_n}. \tag{3}$$

From (3) we immediately get the bound

$$c_n \le \sigma_n^{-1}, \tag{4}$$

and since

$$\sigma_n^{-1} \sim \sqrt{\frac{\pi n}{6}}, \quad \text{as} \quad n \to \infty \tag{5}$$

(see Sect. 2), the theorem asymptotically improves the estimate (2). It is also known (see, e.g., [13]) that

$$\sigma_n = \frac{n}{2^{n-1}} \sum_{0 \le r < n/2,\, r \in \mathbb{Z}} \frac{(-1)^r (n-2r)^{n-1}}{r!\,(n-r)!}.$$

The sequences of numerators and denominators of $\sigma_n/2$ can be found in [16].

Remark 1

(i) Calculation shows that for all $5 \le n \le 1000$ the bound (4) is slightly better than (2).
(ii) For $n \le 4$ the constant σ_n^{-1} in (3) can be replaced by c_n. This follows from the observation that any origin-symmetric convex body in $\mathbb{R}^n$, $n \le 3$, has anomaly 1 (see [17]).

A. Schinzel (personal communication) observed that, with respect to maximum norm, Siegel's lemma can be applied to the following well-known problem from additive number theory. A finite set $\{a_1, \dots, a_n\}$ of integers is called a *sum-distinct set* if any two of its 2^n subsums differ by at least 1. We shall assume, without loss of generality, that $0 < a_1 < a_2 < \cdots < a_n$. In 1955 Erdös and Moser [8, Problem 6] asked for an estimate on the least possible a_n of such a set. They proved that

$$a_n > \max\left\{\frac{2^n}{n}, \frac{2^n}{4\sqrt{n}}\right\} \tag{6}$$

and Erdös conjectured that $a_n > C_0 2^n$, $C_0 > 0$. In 1986 Elkies [7] showed that

$$a_n > 2^{-n}\binom{2n}{n} \tag{7}$$

and this result is still cited by Guy [11, Problem C8] as the best known lower bound for large n. Following [7], note that references [8] and [11] stated the problem equivalently in terms of an "inverse function". They asked one to maximize the size m of a sum-distinct subset of $\{1, 2, \dots, x\}$, given x. Clearly, the bound $a_n > C_1 n^{-s} 2^n$ corresponds to

$$m < \log_2 x + s \log_2 \log_2 x + \log_2 \frac{1}{C_1} - o(1).$$

Corollary 1 *For any sum-distinct set* $\{a_1, \dots, a_n\}$ *with* $0 < a_1 < \cdots < a_n$, *the inequality*

$$a_n > \sigma_n 2^{n-1} \tag{8}$$

holds.

Since

$$2^{-n}\binom{2n}{n} \sim \frac{2^n}{\sqrt{\pi n}} \quad \text{and} \quad \sigma_n 2^{n-1} \sim \frac{2^n}{\sqrt{2\pi n/3}}, \quad \text{as} \quad n \to \infty,$$

Corollary 1 asymptotically improves the result of Elkies with factor $\sqrt{3/2}$.

Remark 2

(i) Sum-distinct sets with a minimal largest element are known up to $n = 9$ (see [5]). In the latter case the estimate (8) predicts $a_9 \geq 116$ and the optimal bound is $a_9 \geq 161$. Calculation shows that for all $10 \leq n \leq 1000$ the bound (8) is slightly better than (7).

(ii) Professor Noam Elkies kindly informed the author about the existence of an unpublished result by him and Andrew Gleason which asymptotically improves (7) with factor $\sqrt{2}$.

2 Sections of the Cube and Sinc Integrals

Let $C = [-1, 1]^n \subset \mathbb{R}^n$ and let $\mathbf{s} = (s_1, \dots, s_n) \in \mathbb{R}^n$ be a unit vector. It is a well-known fact (see, e.g., [2]) that

$$\operatorname{vol}_{n-1}\left(\mathbf{s}^\perp \cap C\right) = \frac{2^n}{\pi} \int_0^\infty \prod_{i=1}^n \frac{\sin s_i t}{s_i t}\, dt, \tag{9}$$

where $\mathbf{s}^\perp$ is the $(n-1)$-dimensional subspace orthogonal to $\mathbf{s}$. In particular, the volume of the section orthogonal to the vertex $\mathbf{v} = (1, \dots, 1)$ of C is given by

$$\operatorname{vol}_{n-1}\left(\mathbf{v}^\perp \cap C\right) = \frac{2^n}{\pi} \int_0^\infty \left(\frac{\sin(t/\sqrt{n})}{t/\sqrt{n}}\right)^n dt = 2^{n-1}\sqrt{n}\,\sigma_n.$$

Laplace and Pólya (see [12, 14] and, e.g., [6]) both gave proofs that

$$\lim_{n\to\infty} \frac{\operatorname{vol}_{n-1}(\mathbf{v}^\perp \cap C)}{2^{n-1}} = \sqrt{\frac{6}{\pi}}.$$

Thus, (5) is justified.

Lemma 1 *For $n \geq 2$,*

$$0 < \sigma_{n+1} < \sigma_n \leq 1.$$

Proof This result is implicit in [4]. Indeed, Theorem 1(ii) of [4] applied with $a_0 = a_1 = \cdots = a_n = 1$ gives the inequalities

$$0 < \sigma_{n+1} \leq \sigma_n \leq 1.$$

The strict inequality $\sigma_{n+1} < \sigma_n$ follows from the observation that in this case the inequality in (3) of [4] is strict with $a_{n+1} = a_0 = y = 1$. □

3 An Application of the Busemann Theorem

Let $|\cdot|$ denote the euclidean norm. Recall that we can associate with each star body L the *distance function* $f_L(\mathbf{x}) = \inf\{\lambda > 0 : \mathbf{x} \in \lambda L\}$. The *intersection body* IL of a star body $L \subset \mathbb{R}^n$, $n \geq 2$, is defined as the $\mathbf{o}$-symmetric star body whose distance function f_{IL} is given by

$$f_{IL}(\mathbf{x}) = \frac{|\mathbf{x}|}{\mathrm{vol}_{n-1}(\mathbf{x}^\perp \cap L)}.$$

Intersection bodies played an important role in the solution to the famous Busemann–Petty problem. The Busemann theorem (see, e.g., Chap. 8 of [9]) states that if L is $\mathbf{o}$-symmetric and convex, then IL is the convex set. This result allows us to prove the following useful inequality. Let $f = f_{IC}$ denote the distance function of IC.

Lemma 2 *For any nonzero* $\mathbf{x} \in \mathbb{R}^n$,

$$f\left(\frac{\mathbf{x}}{\|\mathbf{x}\|}\right) \leq f(\mathbf{v}) = \frac{1}{\sigma_n 2^{n-1}}, \tag{10}$$

with equality only if $n = 2$ *or* $\mathbf{x}/\|\mathbf{x}\|$ *is a vertex of the cube* C.

We proceed by induction on n. When $n = 2$ the result is obvious. Suppose now (10) is true for $n - 1 \geq 2$. Since, if some $x_i = 0$, the problem reduced to that in $\mathbb{R}^{n-1}$, we may assume inductively that $x_i > 0$ for all i. Clearly, we may also assume that $\mathbf{w} = \mathbf{x}/\|\mathbf{x}\|$ is not a vertex of C, in particular, $\mathbf{w} \neq \mathbf{v}$.

Let $Q = [0, 1]^n \subset \mathbb{R}^n$ and let L be the two-dimensional subspace spanned by vectors $\mathbf{v}$ and $\mathbf{x}$. Then $P = L \cap Q$ is a parallelogram on the plane L. To see this, observe that the cube Q is the intersection of two cones $\{\mathbf{y} \in \mathbb{R}^n : y_i \geq 0\}$ and $\{\mathbf{y} \in \mathbb{R}^n : y_i \leq 1\}$ with apexes at the points $\mathbf{o}$ and $\mathbf{v}$, respectively.

Suppose that P has vertices $\mathbf{o}$, $\mathbf{u}$, $\mathbf{v}$, $\mathbf{v} - \mathbf{u}$. Then the edges $\mathbf{ou}$, $\mathbf{ov} - \mathbf{u}$ of P belong to coordinate hyperplanes and the edges $\mathbf{uv}$, $\mathbf{vv} - \mathbf{u}$ lie on the boundary of C. Without loss of generality, we may assume that the point $\mathbf{w}$ lies on the edge $\mathbf{uv}$. Let

$$\mathbf{v}' = \sigma_n \mathbf{v} = \frac{\mathrm{vol}_{n-1}(\mathbf{v}^\perp \cap C)}{2^{n-1}} \frac{\mathbf{v}}{|\mathbf{v}|} \in \frac{1}{2^{n-1}} IC,$$

$$\mathbf{u}' = \sigma_{n-1}\mathbf{u}.$$

Since the point $\mathbf{u}$ lies in one of the coordinate hyperplanes, by the induction hypothesis

$$f(\mathbf{u}') = f(\sigma_{n-1}\mathbf{u}) \leq \frac{1}{2^{n-1}}.$$

Thus, $\mathbf{u}' \in (1/2^{n-1})IC$. Consider the triangle with vertices $\mathbf{o}$, $\mathbf{u}$, $\mathbf{v}$. Let $\mathbf{w}'$ be the point of intersection of segments $\mathbf{ow}$ and $\mathbf{u}'\mathbf{v}'$. Observing that by Lemma 10

$$|\sigma_n \mathbf{w}| < |\mathbf{w}'| < |\sigma_{n-1}\mathbf{w}|,$$

we get

$$\frac{1}{\sigma_{n-1}} < \frac{|\mathbf{w}|}{|\mathbf{w}'|} < \frac{1}{\sigma_n}. \tag{11}$$

By the Busemann theorem IC is convex. Therefore $\mathbf{w}' \in (1/2^{n-1})IC$ and thus

$$|\mathbf{w}'| \le \frac{\mathrm{vol}_{n-1}(\mathbf{w}^\perp \cap C)}{2^{n-1}}.$$

By (11) we obtain

$$f\left(\frac{\mathbf{x}}{\|\mathbf{x}\|}\right) = f(\mathbf{w}) = \frac{|\mathbf{w}|}{\mathrm{vol}_{n-1}(\mathbf{w}^\perp \cap C)} \le \frac{|\mathbf{w}|}{2^{n-1}|\mathbf{w}'|} < \frac{1}{\sigma_n 2^{n-1}}.$$

Applying Lemma 2 to a unit vector $\mathbf{s}$ and using (9) we get the following inequality for sinc integrals.

Corollary 2 *For any unit vector* $\mathbf{s} = (s_1, \dots, s_n) \in \mathbb{R}^n$,

$$\|\mathbf{s}\| \int_0^\infty \prod_{i=1}^n \frac{\sin s_i t}{s_i t}\, dt \ge \int_0^\infty \left(\frac{\sin t}{t}\right)^n dt,$$

with equality only if $n = 2$ *or* $\mathbf{s}/\|\mathbf{s}\|$ *is a vertex of the cube* C.

Remark 3 Note that IC is symmetric with respect to any coordinate hyperplane. This observation and Busemann's theorem immediately imply (10) with nonstrict inequality in all cases.

4 Proof of the Theorem

Clearly, we may assume that $\|\mathbf{a}\| > 1$ and, in particular, that the inequality in Lemma 2 is strict for $\mathbf{x} = \mathbf{a}$. We also assume, without loss of generality, that $\gcd(a_1, \dots, a_n) = 1$.

Let $S = \mathbf{a}^\perp \cap C$ and $\Lambda = \mathbf{a}^\perp \cap \mathbb{Z}^n$. Then S is a centrally symmetric convex set and Λ is an $(n-1)$-dimensional sublattice of $\mathbb{Z}^n$ with determinant (covolume) $\det \Lambda = |\mathbf{a}|$. Let $\lambda_i = \lambda_i(S, \Lambda)$ be the ith successive minimum of S with respect to Λ, that is

$$\lambda_i = \inf\{\lambda > 0 : \dim(\lambda S \cap \Lambda) \ge i\}.$$

By the definition of S and Λ it is enough to show that

$$\lambda_1 \cdots \lambda_{n-1} < \frac{\|\mathbf{a}\|}{\sigma_n}.$$

The $(n-1)$-dimensional subspace $\mathbf{a}^\perp \subset \mathbb{R}^n$ can be considered as a usual $(n-1)$-dimensional Euclidean space. The Minkowski Theorem on Successive Minima (see, e.g. Chap. 2 of [10]), applied to the **o**-symmetric convex set $S \subset \mathbf{a}^{\perp}$ and the lattice $\Lambda \subset \mathbf{a}^{\perp}$, implies that

$$\lambda_1 \cdots \lambda_{n-1} \leq \frac{2^{n-1} \det \Lambda}{\mathrm{vol}_{n-1}(S)} = \frac{2^{n-1}|\mathbf{a}|}{\mathrm{vol}_{n-1}(\mathbf{a}^{\perp} \cap C)} = 2^{n-1} f(\mathbf{a}),$$

and by Lemma 2 we get

$$\lambda_1 \cdots \lambda_{n-1} \leq 2^{n-1} f(\mathbf{a}) = 2^{n-1} f\left(\frac{\mathbf{a}}{\|\mathbf{a}\|}\right)\|\mathbf{a}\| < 2^{n-1} f(\mathbf{v})\|\mathbf{a}\| = \frac{\|\mathbf{a}\|}{\sigma_n}.$$

This proves the theorem.

5 Proof of Corollary 1

For a sum-distinct set $\{a_1, \dots, a_n\}$ consider the vector $\mathbf{a} = (a_1, \dots, a_n)$. Observe that any nonzero integral vector $\mathbf{x}$ with $L(\mathbf{x}) = 0$ must have the maximum norm greater than 1. Therefore (3) implies the inequality

$$2^{n-1} < \frac{\|\mathbf{a}\|}{\sigma_n}.$$

Acknowledgements The author thanks Professors D. Borwein and A. Schinzel for valuable comments and Professor P. Gruber for fruitful discussions and suggestions.

References

1. Aliev, I.: On a decomposition of integer vectors. Ph.D. Dissertation, Institute of Mathematics, PAN, Warsaw (2001)
2. Ball, K.: Cube slicing in $\mathbb{R}^n$. Proc. Am. Math. Soc. **97**(3), 465–472 (1986)
3. Bombieri, E., Vaaler, J.: On Siegel's lemma. Invent. Math. **73**, 11–32 (1983). Addendum. Invent. Math. **75**, 377 (1984)
4. Borwein, D., Borwein, J.: Some remarkable properties of sinc and related integrals. Ramanujan J. **5**(1), 73–89 (2001)
5. Borwein, P., Mossinghoff, M.: Newman polynomials with prescribed vanishing and integer sets with distinct subset sums. Math. Comput. **72**(242), 787–800 (2003); (electronic)
6. Chakerian, D., Logothetti, D.: Cube slices, pictorial triangles, and probability. Math. Mag. **64**(4), 219–241 (1991)
7. Elkies, N.D.: An improved lower bound on the greatest element of a sum-distinct set of fixed order. J. Comb. Theory Ser. A **41**(1), 89–94 (1986)
8. Erdös, P.: Problems and results in additive number theory. In: Colloque sur la Théorie des Nombres, pp. 127–137, Bruxelles (1955)
9. Gardner, R.J.: Geometric Tomography. Encyclopedia of Mathematics and Its Applications, vol. 58. Cambridge University Press, Cambridge (1995)
10. Gruber, P.M., Lekkerkerker, C.G.: Geometry of Numbers. North-Holland, Amsterdam (1987)
11. Guy, R.K.: Unsolved Problems in Number Theory, 3rd edn. Problem Books in Mathematics. Unsolved Problems in Intuitive Mathematics. Springer, New York (2004)
12. Laplace, P.S.: Théorie Analytique des Probabilités. Courcier Imprimeur, Paris (1812)
13. Medhurst, R.G., Roberts, J.H.: Evaluation of the integral $I_n(b) = (2/\pi)\int_0^{\infty}((\sin x)/x)^n \cos(bx)\,dx$. Math. Comput. **19**, 113–117 (1965)
14. Pólya, G.: Berechnung eines Bestimmten Integrals. Math. Ann. **74**, 204–212 (1913)

15. Schinzel, A.: A property of polynomials with an application to Siegel's lemma. Mon.hefte Math. **137**, 239–251 (2002)
16. Sloane, N.J.A.: Sequences A049330 and A049331. In: The On-Line Encyclopedia of Integer Sequences, http://www.research.att.com/~njas/sequences/
17. Woods, A.C.: The anomaly of convex bodies. Proc. Camb. Philos. Soc. **52**, 406–423 (1956)