

# An Improved Upper Bound on the Size of Planar Convex-Hulls<sup>\*</sup>

Abdullah N. Arslan and Ömer Eğecioğlu

Department of Computer Science  
University of California, Santa Barbara  
CA 93106, USA  
{arslan,omer}@cs.ucsb.edu

**Abstract.** Let  $\mathcal{C}$  be the convex-hull of a set of points  $S$  with integral coordinates in the plane. It is well-known that  $|\mathcal{C}| \leq cD^{2/3}$  for some constant  $c$  where  $D$  is the diameter of  $S$ : i.e. the maximum distance between any pair of points in  $S$ . It has been shown that  $c = 7.559..$  for an arbitrary  $S$ , and  $c = 3.496..$  in the special case when  $S$  is a ball centered at the origin in the plane. In this paper we show that  $c = 12/\sqrt[3]{4\pi^2} = 3.524..$  is sufficient for an arbitrary set of lattice points  $S$  of diameter  $D$  in the plane, and  $|\mathcal{C}| \sim 12\sqrt[3]{2/(9\pi^2)} D^{2/3} = 3.388..D^{2/3}$  is achieved asymptotically. Our proof is based on the construction of a special set in first quadrant, and the analysis of the result involves the calculation of the average order of certain number-theoretical functions associated with the Euler totient function  $\phi(n)$ .

## 1 Introduction

A lattice point is a point with integral coordinates. Given a set  $S$  of lattice points in the plane, let  $\mathcal{C}$  be the convex-hull of  $S$ , and denote the number of extreme points in  $\mathcal{C}$  by  $|\mathcal{C}|$ . The behavior of  $|\mathcal{C}|$  as a function of parameters associated with  $S$  has been studied in various contexts in computational geometry, computer graphics [10, 6, 9], and integer programming [1, 3, 5].

Andrews' general theorem [1] on convex bodies in  $d$ -dimensional space implies that in the plane  $|\mathcal{C}|$  is bounded by

$$|\mathcal{C}| \leq cD^{2/3} \tag{1}$$

for some constant  $c$ , where  $D$  is the diameter of  $S$ : i.e. the maximum distance between any two points in  $S$ . Another proof of this bound for the plane was given by Katz and Volper [9]. The constant  $c$  has also been studied. Balog and Bárány [2] showed that when  $S$  is the ball of radius  $r = D/2$  centered at the origin, i.e.  $S = rB^2$ , then

$$0.207..D^{2/3} \leq |\mathcal{C}| \leq 3.496..D^{2/3}.$$

---

<sup>\*</sup> Supported in part by NSF Grant No. CCR-9821038, and a UCSB-COR faculty research grant.

Therefore one can take  $c = 3.496..$  in the special case when  $S$  is a ball of diameter  $D$ . A  $d$ -dimensional analysis for the ball appears in [4]. Har-Peled [7] showed that the value  $c = 6\sqrt[3]{2} = 7.559..$  is sufficient for the bound (1) in the plane for arbitrary  $S$ .

In this paper we investigate further the nature of the constant  $c$  in (1) and show that

$$c = 12/\sqrt[3]{4\pi^2} = 3.524..$$

suffices for an arbitrary  $S$  of diameter  $D$  in the plane. Our proof is based on the construction of a special set in first quadrant of the plane which satisfies certain constraints. The construction involves selecting a set of fractions in a particular order as slopes of the line segments of the convex-hull. Based on the properties of the average order of certain number-theoretical functions associated with the Euler totient function  $\phi(n)$ , we derive an upper bound on the size of the set constructed. This leads to an improved value for  $c$ . We also show that using the construction idea of the proof, we can always create a convex-hull  $\mathcal{C}$  with a given diameter  $D$  such that

$$|\mathcal{C}| \sim 12\sqrt[3]{2/(9\pi^2)} D^{2/3} = 3.388..D^{2/3} \quad (2)$$

is achieved asymptotically.

The organization of this paper is as follows. Section 2 gives the number-theoretical background we require, and includes the proof of the main theorem, which we then use in Section 3 for proving our result on the improved value of  $c$ . In Section 4, we construct large convex-hulls with a given diameter proving (2).

## 2 Number-theoretical definitions and results

We use the classical book by Hardy and Wright [8] as our main reference for the definitions and basic results used in this section. We denote by  $(r, s)$  the greatest common divisor of  $r$  and  $s$ .

- The *Euler totient function*  $\phi(n)$  ([8], p. 52) is defined as follows:
  1.  $\phi(1) = 1$
  2. for  $n > 1$ ,  $\phi(n)$  is the number of positive integers less than  $n$  and relatively prime to  $n$ .
- The *Möbius function*  $\mu(n)$  ([8], p. 234) is defined by
  1.  $\mu(1) = 1$ ,
  2.  $\mu(n) = 0$  if  $n$  has a square factor,
  3.  $\mu(p_1 p_2 \cdots p_k) = (-1)^k$  if all the primes  $p_1, p_2, \dots, p_k$  are different.
- The *Riemann zeta function*  $\zeta(s)$  ([8], p. 245) is defined for  $s > 1$  by

$$\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s} .$$

We use the following well-known results:

**Lemma 1.**

$$\phi(n) = \sum_{d|n} \frac{n}{d} \mu(d), \quad (3)$$

$$\zeta(2)^{-1} = \sum_{d=1}^{\infty} \frac{\mu(d)}{d^2} = \frac{6}{\pi^2}. \quad (4)$$

*Proof.* The proof of (3) is in ([8], p. 235). The proof of (4) can be found in ([8], Thm. 287, p. 250; Thm. 293, p. 251).

Let  $\Phi_0(n) = \phi(1) + \phi(2) + \dots + \phi(n)$ . It is known in relation to Farey fractions ([8], Thm. 330, p. 268) that

$$\Phi_0(n) = \frac{3n^2}{\pi^2} + O(n \log n), \quad (5)$$

so that the *average order* ([8], p. 263) of the function  $\phi(n)$  is given by (5). Theorem 1 below gives an expression for the average order of the function  $n^r \phi(n)$  for  $r \geq 0$ , generalizing (5).

**Theorem 1.** *For any integer  $r \geq 0$*

$$\Phi_r(n) = 1^r \cdot \phi(1) + 2^r \cdot \phi(2) + \dots + n^r \cdot \phi(n) = \frac{6}{(r+2)\pi^2} n^{r+2} + O(n^{r+1} \log n). \quad (6)$$

*Proof.* By (3) of lemma 1 we have

$$\begin{aligned} \Phi_r(n) &= \sum_{m=1}^n m^r \phi(m) = \sum_{m=1}^n m^r \sum_{d|m} \frac{m}{d} \mu(d) = \sum_{m=1}^n \sum_{dd'=m} m^r d' \mu(d) \\ &= \sum_{m=1}^n \sum_{dd'=m} d^r (d')^{r+1} \mu(d) = \sum_{dd' \leq n} d^r (d')^{r+1} \mu(d) = \sum_{d=1}^n d^r \mu(d) \sum_{d'=1}^{\lfloor n/d \rfloor} (d')^{r+1} \end{aligned}$$

Using the fact that

$$\sum_{k=1}^n k^{r+1} = \frac{n^{r+2}}{r+2} + O(n^{r+1}),$$

we get

$$\sum_{d'=1}^{\lfloor n/d \rfloor} (d')^{r+1} = \frac{1}{r+2} \left( \frac{n}{d} \right)^{r+2} + O\left( \frac{n^{r+1}}{d^{r+1}} \right).$$

Therefore

$$\begin{aligned} \Phi_r(n) &= \frac{n^{r+2}}{r+2} \sum_{d=1}^n \frac{\mu(d)}{d^2} + O\left( n^{r+1} \sum_{d=1}^n \frac{1}{d} \right) \\ &= \frac{n^{r+2}}{r+2} \sum_{d=1}^{\infty} \frac{\mu(d)}{d^2} + O\left( n^{r+2} \sum_{d=n+1}^{\infty} \frac{1}{d^2} \right) + O(n^{r+1} \log n) \\ &= \frac{n^{r+2}}{r+2} \zeta(2)^{-1} + O(n^{r+1}) + O(n^{r+1} \log n), \end{aligned}$$

and the theorem follows from the last equality and (4) of lemma 1.

We need the following result relating  $\Phi_0(n)$  and  $\Phi_1(n)$  as a step in our study of  $|\mathcal{C}|$ .

**Theorem 2.** *Let  $\Phi_0(n) = \phi(1) + \phi(2) + \dots + \phi(n)$ ,*  

$$\Phi_1(n) = 1 \cdot \phi(1) + 2 \cdot \phi(2) + \dots + n \cdot \phi(n).$$

*Then*

$$\Phi_0(n) \sim \frac{3}{\sqrt[3]{4\pi^2}} \Phi_1(n)^{2/3} = 0.8810516.. \Phi_1(n)^{2/3}. \quad (7)$$

*Proof.* The theorem follows by combining the expressions for  $\Phi_0(n)$  and  $\Phi_1(n)$  obtained as the cases  $r = 0$ , and  $r = 1$  of theorem 1.

We note that also the magnitude of the error term in (7) can be calculated by using the full expressions for  $\Phi_0(n)$  and  $\Phi_1(n)$  obtained. This gives

$$\Phi_0(n) = \frac{3}{\sqrt[3]{4\pi^2}} \Phi_1(n)^{2/3} + O\left(\Phi_1(n)^{1/3} \log \Phi_1(n)\right).$$

We omit the details of this calculation.

### 3 An improved upper bound

We first establish an upper bound on the size of the convex-hull of lattice points in first quadrant of the plane in the following lemma.

**Lemma 2.** *Let  $S_{a,b}$  be a set of lattice points in first quadrant of the  $xy$ -plane enclosed by  $y = a$  and  $x = b$ . For the convex-hull  $\mathcal{C}_{a,b}$  of  $S_{a,b}$ , there holds*

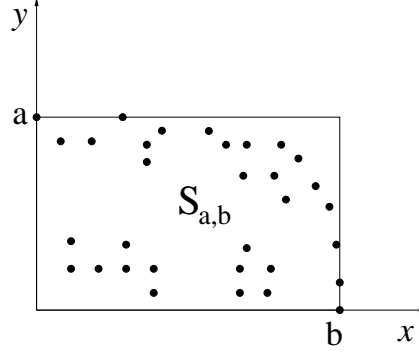
$$|\mathcal{C}_{a,b}| \leq \frac{3}{\sqrt[3]{4\pi^2}} (a+b)^{2/3} + O\left((a+b)^{1/3} \log(a+b)\right)$$

*Proof.* Without loss of generality,  $S_{a,b}$  includes the points  $(0, a)$  and  $(b, 0)$  and both  $a$  and  $b$  are positive integers (Figure 1). Instead of the point-set  $\mathcal{C}_{a,b}$  we consider the corresponding set of slopes  $\mathcal{R}_{a,b}$  of the line segments (edges) connecting the consecutive extreme points of the convex-hull. Clearly,  $|\mathcal{C}_{a,b}| = |\mathcal{R}_{a,b}| + 1$ , so we can alternately study the properties of the set  $\mathcal{R}_{a,b}$ . By convexity, the slopes of the edges of the convex-hull are all different. Furthermore  $S_{a,b}$  is a set of lattice points, and therefore the slopes of the non-vertical edges are all rational numbers.

Let  $\mathcal{R}_{a+b}^*$  be an optimal set for the following problem: maximize  $|\mathcal{R}|$  subject to

$$\sum_{\frac{y}{x} \in \mathcal{R}} y + \sum_{\frac{y}{x} \in \mathcal{R}} x = \sum_{\frac{y}{x} \in \mathcal{R}} y + x \leq a + b \quad (8)$$

Clearly, for any  $a$  and  $b$ ,  $|\mathcal{R}_{a,b}| \leq |\mathcal{R}_{a+b}^*|$ . We will find a bound for  $|\mathcal{R}_{a+b}^*|$ . Let  $\mathcal{Q}_i$  for  $i \geq 0$  be the set of slopes defined as follows:



**Fig. 1.** A set of lattice points  $S_{a,b}$  in first quadrant.

1.  $\mathcal{Q}_0 = \emptyset$ ,
2.  $\mathcal{Q}_1 = \left\{ \frac{0}{1}, \frac{1}{0} \right\}$ . We assume that the fraction  $\frac{1}{0}$  is defined as a slope and it represents the vertical edge whose length is one unit.
3. For  $i > 1$ ,  $\mathcal{Q}_i = \left\{ \frac{y}{x} \mid y + x = i \text{ and } (y, x) = 1 \right\}$ .

Table 1 illustrates the first few values  $\mathcal{Q}_i$ ,  $\phi(i)$ ,  $\Phi_0(i)$ , and  $\Phi_1(i)$ . The following properties can easily be seen for  $i > 1$ :

$$|\mathcal{Q}_i| = \phi(i) \tag{9}$$

$$\sum_{\frac{y}{x} \in \mathcal{Q}_i} y + x = i |\mathcal{Q}_i| \tag{10}$$

Let  $n + 1$  be the smallest number such that  $\sum_{i=1}^{n+1} i |\mathcal{Q}_i| > a + b$ , and  $\mathcal{Q}'_{n+1}$  be an arbitrary subset of  $\mathcal{Q}_{n+1}$  such that

$$|\mathcal{Q}'_{n+1}| = \left\lfloor \frac{(a + b) - \sum_{i=1}^n i |\mathcal{Q}_i|}{n + 1} \right\rfloor$$

Then consider the following set

$$\mathcal{R}_{a+b} = \left( \bigcup_{i=1}^n \mathcal{Q}_i \right) \cup \mathcal{Q}'_{n+1}. \tag{11}$$

We claim that  $\mathcal{R}_{a+b}$  is a maximal set which satisfies the constraint (8). The expression (11) describes a greedy construction : To include in set  $\mathcal{R}_{a+b}$ , select a fraction whose numerator-denominator sum is the smallest. Continue including fractions until the sum of all the numerators and the denominators of the fractions currently in the set exceeds  $a + b$  . Since  $\mathcal{R}_{a+b}$  is a set, no fraction can be included in the set more than once, and since the slopes are all different, among the equivalent fractions, the irreducible one has the smallest numerator-denominator sum. This explains why only the relatively prime numbers are to be considered in the construction.

$i$	$\mathcal{Q}_i$	$\phi(i)$	$\Phi_0(i)$	$\Phi_1(i)$
1	$\{\frac{0}{1}, \frac{1}{0}\}$	1	1	1
2	$\{\frac{1}{1}\}$	1	2	3
3	$\{\frac{1}{2}, \frac{2}{1}\}$	2	4	9
4	$\{\frac{1}{3}, \frac{3}{1}\}$	2	6	17
5	$\{\frac{1}{4}, \frac{2}{3}, \frac{3}{2}, \frac{4}{1}\}$	4	10	37
6	$\{\frac{1}{5}, \frac{5}{1}\}$	2	12	49
7	$\{\frac{1}{6}, \frac{2}{5}, \frac{3}{4}, \frac{4}{3}, \frac{5}{2}, \frac{6}{1}\}$	6	18	91

**Table 1.** Table of  $\mathcal{Q}_i$ ,  $\phi(i)$ ,  $\Phi_0(i)$ , and  $\Phi_1(i)$  for  $i = 1, 2, \dots, 7$ .

From (11) we have

$$\bigcup_{i=1}^n \mathcal{Q}_i \subseteq \mathcal{R}_{a+b} \subseteq \bigcup_{i=1}^{n+1} \mathcal{Q}_i \quad (12)$$

Using (12) and (9) we find that

$$\sum_{i=1}^n \phi(i) + 1 \leq |\mathcal{R}_{a+b}| \leq \sum_{i=1}^{n+1} \phi(i) + 1 \quad (13)$$

Again using (12) and (9) together with the expression (10), and using the fact that by construction  $n+1$  is the smallest number such that  $\sum_{i=1}^{n+1} i|\mathcal{Q}_i| > a+b$  we get

$$\sum_{i=1}^n i\phi(i) + 1 \leq a+b \leq \sum_{i=1}^{n+1} i\phi(i) + 1 \quad (14)$$

We note that  $\phi(n+1) = O(\Phi_1(n)^{1/3})$  using the expression  $\Phi_1(n)$  obtained from (6) with  $r=1$ . Therefore we can write the following upper bound for  $|\mathcal{R}_{a+b}|$  using (13):

$$|\mathcal{R}_{a+b}| = \sum_{i=1}^n \phi(i) + O(\Phi_1(n)^{1/3}) = \Phi_0(n) + O(\Phi_1(n)^{1/3})$$

Furthermore from Theorem 2

$$|\mathcal{R}_{a+b}| = \frac{3}{\sqrt[3]{4\pi^2}} \Phi_1(n)^{2/3} + O(\Phi_1(n)^{1/3} \log \Phi_1(n)) + O(\Phi_1(n)^{1/3}), \quad (15)$$

and from (14) we obtain that  $\Phi_1(n) \sim a+b$ . Therefore

$$|\mathcal{R}_{a+b}| = \frac{3}{\sqrt[3]{4\pi^2}} (a+b)^{2/3} + O((a+b)^{1/3} \log(a+b))$$

which proves the bound for  $|\mathcal{C}_{a,b}|$  of the lemma.

**Theorem 3.** For the convex-hull  $\mathcal{C}$  of a set  $S$  of lattice points of diameter  $D$  in the plane, there holds

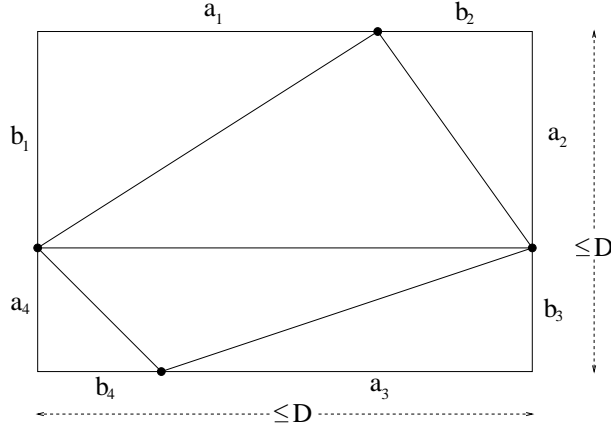
$$|\mathcal{C}| \leq \frac{12}{\sqrt[3]{4\pi^2}} D^{2/3} + O\left(D^{1/3} \log D\right)$$

*Proof.*  $S$  can be enclosed by an axis-parallel rectangle whose sides are at most  $D$  in length. Using this rectangle, we can partition  $S$  into four parts such that each part is confined to a single quadrant as shown in Figure 2. For the size of  $\mathcal{C}$  we have

$$|\mathcal{C}| \leq |\mathcal{C}_{a_1, b_1}| + |\mathcal{C}_{a_2, b_2}| + |\mathcal{C}_{a_3, b_3}| + |\mathcal{C}_{a_4, b_4}|$$

By Lemma 2 we can rewrite the inequality as

$$|\mathcal{C}| \leq \frac{3}{\sqrt[3]{4\pi^2}} ((a_1+b_1)^{2/3} + (a_2+b_2)^{2/3} + (a_3+b_3)^{2/3} + (a_4+b_4)^{2/3}) + O\left(D^{1/3} \log D\right) \quad (16)$$



**Fig. 2.** Partitions of  $S$  in quadrants.

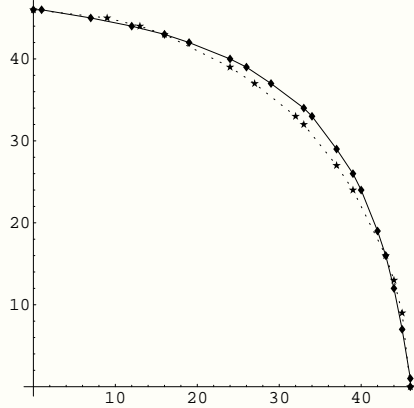
The function  $f(x) = x^{2/3}$  is concave on  $[0, \infty)$ . In particular for nonnegative  $x_1$  and  $x_2$ ,

$$x_1^{2/3} + x_2^{2/3} \leq 2 \left( \frac{x_1 + x_2}{2} \right)^{2/3}.$$

Therefore, the equality in (16) becomes

$$|\mathcal{C}| \leq \frac{3}{\sqrt[3]{4\pi^2}} 4 \left( \frac{a_1 + b_1 + a_2 + b_2 + a_3 + b_3 + a_4 + b_4}{4} \right)^{2/3} + O\left(D^{1/3} \log D\right)$$

Since  $a_1 + b_2$ ,  $a_3 + b_4$ ,  $a_2 + b_3$ , and  $a_4 + b_1$  are all smaller than or equal to  $D$ , the inequality for  $|\mathcal{C}|$  of the theorem holds.



**Fig. 3.**  $n = 7$ ,  $a = b = 46 = \frac{1}{2}\Phi_1(7) + \frac{1}{2}$ . The dotted line is used for the convex-hull of the set of lattice points in the ball of radius 46 in first quadrant. The solid lines show the constructed hull  $\mathcal{C}(7)$ .

#### 4 Constructing a large convex-hull with a given diameter

To investigate how tight the new value of  $c$  in the upper bound for  $|\mathcal{C}|$  is, we revisit the proof of Lemma 2. We first describe how we can actually construct a convex-hull  $\mathcal{C}_{a+b}$  from the set of slopes  $\mathcal{R}_{a+b}$  created in the proof for particular  $a$  and  $b$ . More precisely, for every  $n$ , we construct a convex-hull  $\mathcal{C}(n)$  in first quadrant with  $a = b = \frac{1}{2}\Phi_1(n) + \frac{1}{2}$ , symmetric about the line  $y = x$ . As its set of slopes, we take

$$\mathcal{R}(n) = \bigcup_{i=1}^n \mathcal{Q}_i.$$

$\mathcal{C}(n)$  connects the point  $(0, \frac{1}{2}\Phi_1(n) + \frac{1}{2})$  on the  $y$ -axis to  $(\frac{1}{2}\Phi_1(n) + \frac{1}{2}, 0)$  on the  $x$ -axis and consists of  $\Phi_0(n)$  edges. We start with the point  $(0, \frac{1}{2}\Phi_1(n) + \frac{1}{2})$  as the first vertex, and if the  $i$ -th smallest fraction in  $\mathcal{R}(n)$  is  $y_i/x_i$ , then we place the next vertex on the hull  $x_i$  units to the right and  $y_i$  units down from the current vertex. See Figure 4 for the  $n = 5$  case.

Now consider the  $\mathcal{C}(n)$  constructed as we described. If it includes a vertex whose distance from the origin is larger than  $\frac{1}{2}\Phi_1(n) + \frac{1}{2}$ , then the diameter of the set constructed by taking four copies of  $\mathcal{C}(n)$  around the origin will have diameter larger than  $D$ . That this is indeed the case can be seen from Figure 3, where the point farthest from the origin in our construction is not inside the ball with radius 46. Thus the constant  $c = 12/\sqrt[3]{4\pi^2} = 3.352..$  in the upper bound is not tight.

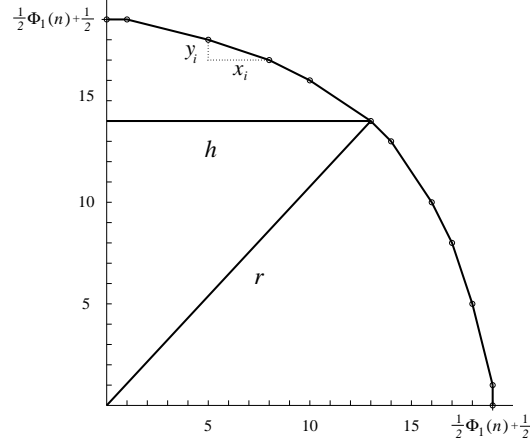
We next investigate how close we can come to this value. It follows by symmetry and convexity that the farthest vertex from the origin on  $\mathcal{C}(n)$  constructed is one of the endpoints of the edge with slope 1 on the hull as shown in Figure 4. Denote by  $h(n)$  the  $x$ -coordinate of this point, and by  $r(n)$  its distance from



the origin. By construction

$$h(n) = \sum_{i+j \leq n} j \chi[(i, j) = 1] \chi[i \leq j] = \sum_{j=1}^n j \sum_{i=1}^j \chi[(i, j) = 1] \chi[i + j \leq n] \quad (17)$$

where  $\chi$  is the indicator function of its argument, i.e., it is 1 if its argument evaluates to true, and 0 otherwise.



**Fig. 4.**  $n = 5$ ,  $a(n) = b(n) = \frac{1}{2}\Phi_1(5) + \frac{1}{2} = 19$ .

We next show that  $h(n) \sim \frac{3}{8}\Phi_1(n)$ . Since intercepts of the hull are  $a(n) = b(n) = \frac{1}{2}\Phi_1(n) + \frac{1}{2}$  this implies  $h(n) \sim \frac{3}{4}a(n)$ , and we can calculate  $r(n)$  by the Pythagorean formula as

$$r(n) \sim \frac{3\sqrt{2}}{4}a(n). \quad (18)$$

**Theorem 4.** *Suppose  $h(n)$  is as defined in (17), and  $\Phi_1(n)$  as defined in Theorem 2. Then  $h(n) = \frac{3}{8}\Phi_1(n) + O(n^2 \log n)$ .*

*Proof.* We will indicate the derivation of the asymptotic part and ignore the calculation of the error terms. First we write  $h(n) = h_1(n) + h_2(n)$  where in  $h_1(n)$ , the index  $j$  runs from 1 to  $n/2$ , and in  $h_2$ ,  $j$  runs from  $n/2 + 1$  to  $n$ . Then

$$h_1(n) = \sum_{j=1}^{\frac{n}{2}} j \sum_{i=1}^j \chi[(i, j) = 1],$$

since for the indices in question  $i \leq j$  and we automatically have  $i + j \leq n$ . Therefore  $h_1(n) = \Phi_1(\frac{n}{2})$ . On the other hand, if  $j \geq n/2$ , then  $n - j \leq j$  and

$$h_2(n) = \sum_{j=\frac{n}{2}}^n j \sum_{i=1}^j \chi[(i, j) = 1] \chi[i \leq n - j]$$

$$\sim \sum_{j=\frac{n}{2}}^n j \cdot \frac{n-j}{j} \phi(j) \sim n \left( \Phi_0(n) - \Phi_0\left(\frac{n}{2}\right) \right) - \left( \Phi_1(n) - \Phi_1\left(\frac{n}{2}\right) \right).$$

Using the expressions  $\Phi_0(n) \sim 3n^2/\pi^2$ , and  $\Phi_1(n) \sim 2n^3/\pi^2$  from Theorem 2, and adding the terms for  $h_1(n)$  and  $h_2(n)$ , we obtain

$$h(n) \sim \left( \frac{1}{4} + 3 - \frac{3}{4} - 2 + \frac{1}{4} \right) \frac{n^3}{\pi^2} = \frac{3n^3}{4\pi^2} \sim \frac{3}{8} \Phi_1(n)$$

as claimed.

**Theorem 5.** *For  $D$  large, there exists a set of lattice points in the plane with diameter  $D$  and convex-hull  $\mathcal{C}$  such that*

$$|\mathcal{C}| \sim 12 \sqrt[3]{\frac{2}{9\pi^2}} D^{2/3} = 3.388..D^{2/3}.$$

*Proof.* If we set  $a = b = \frac{2}{3\sqrt{2}} D$  where  $D$  is of the form  $\Phi_1(n)$ , and use the construction for  $\mathcal{C}(n)$ , then  $r \sim D/2$  by (18). By Lemma 2

$$|\mathcal{C}(n)| \sim \frac{3}{\sqrt[3]{4\pi^2}} \left( \frac{4}{3\sqrt{2}} \right)^{2/3} D^{2/3} = 3 \sqrt[3]{\frac{2}{9\pi^2}} D^{2/3}. \quad (19)$$

Since identical convex-hulls are constructed in all four quadrants to obtain  $\mathcal{C}$  from  $\mathcal{C}(n)$ , the diameter of  $\mathcal{C}$  is  $D$  and  $|\mathcal{C}| \sim 4|\mathcal{C}(n)|$ . This proves the claim of the theorem when combined with (19).

## References

1. George E. Andrews. An asymptotic expression for the number of solutions of a general class of diophantine equations. *Transactions of the AMS* 99:272–277, May 1961.
2. B. Balog and I. Bárány. On the convex hull of integer points in a disc. *DIMACS Series, Discrete and Computational Geometry*, 6:39–44, 1991.
3. I. Bárány, R. Howe, and L. Lovasz. On integer points in polyhedra: a lower bound. *Combinatorica*, 12:135–142, 1992.
4. I. Bárány and David G. Larman. The convex hull of integer points in a large ball. *Math. Ann.*, 312:167–181, 1998.
5. W. Cook, M. Hartman, R. Kannan, and C. McDiarmid. On integer points in polyhedra. *Combinatorica*, 12:27–37, 1992.
6. A. Efrat and C. Gotsman. Subpixel image registration using circular fiducials. *Internat. J. Comput. Geom. Appl.*, 4(4):403–422, 1994.
7. S. Har-Peled. An output sensitive algorithm for discrete convex hulls. *Computational Geometry*, 10:125–138, 1998.
8. G. H. Hardy and E. M. Wright. *An introduction to the theory of numbers*. Oxford University Press, April 1980.
9. M. D. Katz and D. J. Volper. Data structures for retrieval on square grids. *SIAM J. Comput.*, 15(4):919–931, November 1986.
10. A. M. Vershik. On the number of convex lattice polytopes. *Geometry and Functional Analysis*, 2:381–393, 1992.