B. Sury, M. Vsemirnov *Res. Number Theory (2022)8:39*
https://doi.org/10.1007/s40993-022-00338-5

Research in Number Theory

RESEARCH

Packing polynomials on irrational sectors

B. Sury[1*] and M. Vsemirnov[2]

[*]Correspondence:
surybang@gmail.com
[1]Statistics & Mathematics Unit, Indian Statistical Institute, 8th Mile Mysore Road, Bangalore 560059, India
Full list of author information is available at the end of the article

Abstract

Fueter and Polya proved that the only quadratic polynomials giving a bijection between N and N^2 are the two Cantor polynomials. It is conjectured that there is no bijection from N^2 onto N given by a polynomial of degree at least 3. A similar problem arises when the domain of the map is replaced by the set of integral points in some sector in R^2. Rational sectors were considered by Nathanson and Stanton. Here, we study and solve the case of general irrational sectors. In fact, our method enables us also to recover the results on rational sectors and also answer a question posed by Nathanson.

Keywords: Cantor polynomials, Irrational sectors, Packing polynomials

Mathematics Subject Classification: 05A15, 11B34, 52C15

1 Introduction

In his seminal works [1,2] which developed the foundations of modern set theory, Cantor established, in particular, a bijection between the set $\mathbb{N}$ of non-negative integers and $\mathbb{N}^2$. In [4], Fueter and Polya established that the only quadratic polynomials that bijectively map $\mathbb{N}^2$ onto $\mathbb{N}$ are the two Cantor polynomials

$$\frac{(x+y)^2+3x+y}{2} \quad \text{and} \quad \frac{(x+y)^2+x+3y}{2}.$$

The original proof was rather complicated, using deep tools from analytic number theory, such as Lindemann's transcendence theorem. An elementary proof was given in [13]. More generally, an explicit polynomial bijection between $\mathbb{N}^r$ and $\mathbb{N}$ for any $r \geq 2$, is given (see [3]) by the map

$$F(x_1, x_2, \dots, x_r) = x_1 + \binom{x_1+x_2+1}{2} + \cdots + \binom{x_1+x_2+\cdots+x_r+r-1}{r}.$$

There are several ways to generalize the two-dimensional problem. It is conjectured that there is no bijection from $\mathbb{N}^2$ onto $\mathbb{N}$ given by a polynomial of degree $d \geq 3$. The cases $d = 3, 4$ were settled by Lew and Rosenberg [7,8]. Higher-degree case remains an open problem. A similar problem arises when the domain of the map is replaced by the set of integral points in some sector in $\mathbb{R}^2$. Rational sectors were considered by Nathanson [9,10] and Stanton [12]. Here, we study and solve the cases of general *irrational sectors*. In fact, our method enables us also to recover the results on rational sectors and also answer a question (Question 6) posed by Nathanson [9].

Springer

After submission of the paper the authors became aware that the question of Nathanson was independently settled in [5] by a different method. The authors are grateful to an anonymous referee for pointing out the corresponding reference.

2 Notations and statement of main results

Let $0 \le \alpha < \beta \le \infty$ be fixed. Consider

$$\mathbb{S} = \mathbb{S}^{\alpha,\beta} = \{(x, y) \in \mathbb{R}^2 : x \ge 0,\ \alpha x \le y \le \beta x\}, \tag{1}$$

$$\mathbb{S}_{\mathbb{Z}} = \mathbb{S}_{\mathbb{Z}}^{\alpha,\beta} = \mathbb{S}^{\alpha,\beta} \cap \mathbb{Z}^2. \tag{2}$$

Definition 1 We say that the sector $\mathbb{S}^{\alpha,\beta}$ is *rational* if α is rational and β is either rational or ∞. Otherwise we call the sector $\mathbb{S}^{\alpha,\beta}$ *irrational.*

Definition 2 The ray $\{(\mu t, \nu t)) : t \in \mathbb{R}_{>0}\}$ is said to be *rational* if it contains a rational point. Otherwise, we call it *irrational.*

Let P be a quadratic polynomial in two variables X and Y with real coefficients. We write

$$P = a_{20}X^2 + a_{11}XY + a_{02}Y^2 + a_{10}X + a_{01}Y + a_{00} \tag{3}$$

and set

$$P_2 = a_{20}X^2 + a_{11}XY + a_{02}Y^2, \tag{4}$$

$$P_1 = a_{10}X + a_{01}Y, \tag{5}$$

so that $P = P_2 + P_1 + a_{00}$.

Definition 3 Finally, we say that P is a quadratic *packing polynomial on* $\mathbb{S}$ if it induces a bijection $P : \mathbb{S}_{\mathbb{Z}} \to \mathbb{N}$ (as mentioned in the introduction, in our notation, $\mathbb{N}$ contains 0).

For any nonnegative integer n we define

$$\mathbb{S}(n) = \{(x, y) \in \mathbb{S} : 0 \le P(x, y) < n\}. \tag{6}$$

In particular, if P is a packing polynomial on $\mathbb{S}$, then

$$|\mathbb{S}(n) \cap \mathbb{Z}^2| = n. \tag{7}$$

With the above notations, the main result is:

Theorem 1 *If P is a quadratic packing polynomial on $\mathbb{S} = \mathbb{S}^{\alpha,\beta}$, then for some integers $d > 0$, u and v with $(u, v) = 1$ we have*

$$2a_{20} = du^2, \quad a_{11} = duv, \quad 2a_{02} = dv^2.$$

Moreover,

$$2a_{20}\beta^{-1} + a_{11}(1 + \alpha\beta^{-1}) + 2a_{02}\alpha = 1 - \alpha\beta^{-1}. \tag{8}$$

The above relation is also valid for the sector with $\beta = \infty$ if we set $\beta^{-1} = 0$.

As a corollary, we obtain Stanton's necessary condition for rational sectors.

Corollary 1 *Let $\alpha = 0$ and $\beta = n/m$ with integers $n, m \ge 1$, $(m, n) = 1$. If P is a quadratic packing polynomial on $\mathbb{S}^{0,n/m}$, then $n \mid (1 - m)^2$ and*

$$P_2(X, Y) = \frac{n}{2}\left(X + \frac{1 - m}{n}Y\right)^2.$$

As another corollary of the theorem, noting that (8) cannot hold if $\alpha = 0$ and β is irrational, we obtain an affirmative answer to a question (Question 6) posed by Nathanson in [9].

Corollary 2 *There exists no packing polynomial on $\mathbb{S}^{0,\beta}$ for any positive, irrational number β.*

For any fixed polynomial $P \in \frac{1}{2}\mathbb{Z}[X, Y]$ and any odd $p \in \mathbb{N}$ and $k \in \mathbb{Z}$ we define $N(p, k)$ as the number of residue classes satisfying the congruence

$$P(x, y) \equiv k \pmod{p}, \tag{9}$$

i.e.,

$$N(p, k) = |\{(x, y) : 0 \le x, y < p,\ P(x, y) \equiv k \pmod{p}\}|. \tag{10}$$

The following theorem is the main technical ingredient of our proofs.

Theorem 2 *Let P be a quadratic packing polynomial on $\mathbb{S}$. For any odd positive integer p and any integer k, we have $N(p, k) = p$.*

3 Some preliminary results

Lemma 1 *If P takes integer values on $\mathbb{S}_{\mathbb{Z}}$, then the numbers a_{11}, $2a_{20}$, $2a_{02}$, $2a_{10}$, $2a_{01}$, $a_{20} + a_{10}$, $a_{02} + a_{01}$, and a_{00} are integers.*

Proof There exist integers u and v such that the nine points $(u+i, v+j)$ with $i, j \in \{0, 1, 2\}$ lie in $\mathbb{S}_{\mathbb{Z}}$. We have

$$\begin{aligned}
a_{11} &= P(u+1, v+1) - P(u+1, v) - P(u, v+1) + P(u, v),\\
2a_{20} &= P(u+2, v) - 2P(u+1, v) + P(u, v),\\
2a_{02} &= P(u, v+2) - 2P(u, v+1) + P(u, v),\\
2a_{10} &= -(2u+1)P(u+2, v) - 2vP(u+1, v+1) + (4u+2v+4)P(u+1, v)\\
&\quad +2vP(u, v+1) - (2u+2v+3)P(u, v),\\
2a_{01} &= -(2v+1)P(u, v+2) - 2uP(u+1, v+1) + (2u+4v+4)P(u, v+1)\\
&\quad +2uP(u+1, v) - (2u+2v+3)P(u, v),\\
a_{20} + a_{10} &= -uP(u+2, v) - vP(u+1, v+1) + (2u+v+1)P(u+1, v)\\
&\quad +vP(u, v+1) - (u+v+1)P(u, v),\\
a_{02} + a_{01} &= -vP(u, v+2) - uP(u+1, v+1) + (u+2v+1)P(u, v+1)\\
&\quad +uP(u+1, v) - (u+v+1)P(u, v),\\
a_{00} &= \binom{u+1}{2}P(u+2, v) + uvP(u+1, v+1) - (u^2+uv+2u)P(u+1, v)\\
&\quad +\binom{v+1}{2}P(u, v+2) - (v^2+uv+2v)P(u, v+1)\\
&\quad +\left(\binom{u+1}{2} + \binom{v+1}{2} + uv + u + v + 1\right)P(u, v),
\end{aligned}$$

and the claim follows. □

4 Reducibility of P_2

Lemma 2 ([13, Lemma 2.4], [10, Lemma 2]) *For any integer $\ell \neq 0$ and any integer non-square D, there is a prime p such that D is a quadratic non-residue modulo p and $p \nmid \ell D$.*

Remark 1 There is a slight inaccuracy in the proof of [10, Lemma 2]. In the notation of [10], one must choose p that additionally satisfies $p \nmid m$.

Lemma 3 *Let P be a packing polynomial on $\mathbb{S}$, and let P_2 be as above. Consider the discriminant of P_2:*

$$D = a_{11}^2 - 4a_{20}a_{02}. \tag{11}$$

We have that D is the square of an integer. In particular, P_2 factorizes over $\mathbb{Q}$ into a product of two linear (not necessarily distinct) polynomials.

Remark 2 For similar results stated for $\mathbb{S}^{0,\infty}$, see also [13, p. 709, proof of Proposition 2.1] and [10, Lemma 6]).

Proof (Proof of Lemma 3) Let us set

$$U = 4a_{20}X + 2a_{11}Y + 2a_{10},$$
$$V = 2DY + 2a_{11}a_{10} - 4a_{20}a_{01}.$$

By Lemma 1, D is an integer and U, V are polynomials in X, Y with integer coefficients. A straightforward but a bit tedious computation gives us

$$16a_{20}DP = DU^2 - V^2 + r, \tag{12}$$

where

$$r = 16Da_{20}a_{00} - 4Da_{10}^2 + (2a_{11}a_{10} - 4a_{20}a_{01})^2. \tag{13}$$

Applying Lemma 1 again we conclude that r is an integer.

Assume that D is not an integer square. In particular, $a_{20} \neq 0$. By Lemma 2, we can find a prime p such that $p \nmid 16a_{20}D$ and $\left(\frac{D}{p}\right) = -1$. Now we prove that if

$$16a_{20}DP(x, y) \equiv r \pmod{p} \tag{14}$$

for some integers x, y, then

$$16a_{20}DP(x, y) \equiv r \pmod{p^2}. \tag{15}$$

In particular, P never takes values congruent to $p + (16a_{20}D)^{-1}r$ modulo p^2; here $(16a_{20}D)^{-1}$ denotes the multiplicative inverse of $16a_{20}D$ modulo p^2. Hence, P cannot be onto $\mathbb{N}$.

Indeed, if (14) holds then (12) gives us $DU(x, y)^2 - V(x, y)^2 \equiv 0 \pmod{p}$. Since D is a quadratic non-residue modulo p, the last congruence holds only if $p \mid U(x, y)$, $p \mid V(x, y)$. Hence, $p^2 \mid DU(x, y)^2 - V(x, y)^2$ and (15) holds.

Thus, D must be a square. The final claim is now obvious.

□

5 Positivity of P_2

Lemma 4 *Let P, P_2 and P_1 be as in (3)–(5), respectively. Assume further that P takes nonnegative integer values on $\mathbb{S}_{\mathbb{Z}}$. If P_2 vanishes on some rational ray in $\mathbb{S}$, then P is not injective on $\mathbb{S}_{\mathbb{Z}}$.*

Proof Clearly, integer-valued linear functions in two variables are not injective on $\mathbb{S}_{\mathbb{Z}}$. Indeed, the number of points in $\mathbb{S}_{\mathbb{Z}} \cap [0, M]^2$ grows quadratically with respect to M, while the size of

$$\mathbb{Z} \cap \{a_{10}x + a_{01}y + a_{00} : (x, y) \in \mathbb{S}_{\mathbb{Z}} \cap [0, M]^2\}$$

is bounded by some linear function in M.

Thus, it is enough to consider the case when P_2 is not identically 0. Moreover, since

$$0 \leq P(xz, yz) = z^2 P_2(x, y) + zP_1(x, y) + a_{00}$$

for any $(x, y) \in \mathbb{S}_{\mathbb{Z}}$ and $z \in \mathbb{N}$, we have that P_2 is nonnegative on any rational ray in $\mathbb{S}$.

Assume that P_2 vanishes on some rational ray in $\mathbb{S}$. In particular, any rational ray contains infinitely many integer points, so we have $P_2(u, v) = 0$ for some non-negative integers u and v, $(u, v) \in \mathbb{S}_{\mathbb{Z}}$, $(u, v) \neq (0, 0)$. Therefore, $P(ut, vt) = t(a_{10}u + a_{01}v) + a_{00}$. Put $m = a_{10}u + a_{01}v = P(u(t + 1), v(t + 1)) - P(ut, vt)$. In particular, m is an integer.

Since P takes nonnegative integer values on $\mathbb{S}_{\mathbb{Z}}$, we have that $P(ut, vt) = mt + a_{00}$ is non-negative for any positive integer t. Therefore, $m \geq 0$. If $m = 0$ then P is not injective, since $P(ut, vt) = a_{00}$ for any positive integer t. Thus, we may assume that $m > 0$.

Now we specify the value of t. Since P_2 is not identically 0, by the observation at the beginning of the proof we can find $(r, s) \in \mathbb{S}_{\mathbb{Z}}$ such that $P_2(r, s) > 0$. Moreover, we may choose them in such a way that

$$P_2(2r, 2s) > 2|a_{10}r + a_{01}s| \tag{16}$$

(otherwise replace (r, s) by $(r\ell, s\ell)$ for a sufficiently large scale factor ℓ). We have

$$P(2rm, 2sm) = m(4a_{20}r^2m + 4a_{11}rsm + 4a_{02}s^2m + 2a_{10}r + 2a_{01}s) + a_{00}.$$

Set

$$t = 4a_{20}r^2m + 4a_{11}rsm + 4a_{02}s^2m + 2a_{10}r + 2a_{01}s = mP_2(2r, 2s) + 2a_{10}r + 2a_{01}s$$

By Lemma 1, t is an integer, and $t > 0$ by (16), so that both (ut, vt) and $(2rm, 2sm)$ are in $\mathbb{S}_{\mathbb{Z}}$. On the other hand,

$$P(ut, vt) = mt + a_{00} = P(2rm, 2sm).$$

Since $P_2(u, v) = 0$ but $P_2(r, s) \neq 0$ and P_2 is homogeneous, we have that (r, s) is not proportional to (u, v), hence $(2rm, 2sm) \neq (ut, vt)$. Therefore, P is not injective. □

Corollary 3 *If P be a quadratic packing polynomial on $\mathbb{S}_{\mathbb{Z}}$ then $P_2(u, v) > 0$ for any $(u, v) \in \mathbb{S} \setminus \{(0, 0)\}$.*

Proof Lemma 3 implies that P_2 does not vanish on irrational rays, while Lemma 4 says that P_2 does not vanish on rational rays in $\mathbb{S}$. □

6 Equidistribution modulo *p*

The aim of this section is to prove Theorem 2, namely, to show that for a quadratic packing polynomial P on $\mathbb{S}$ and any odd $p \in \mathbb{N}$ the number of residue classes satisfying $P(x, y) \equiv k \pmod{p}$ is independent of k. Note that oddness of p is needed in the arguments below because $P(x + ap, y + bp) \equiv P(x, y) \pmod{p}$ is true for odd p, and may not be true for even p since one may have 2 as the common denominator of the coefficients of P.

We need several auxiliary results. By Corollary 3, P_2 is positive on $\mathbb{S} \setminus \{(0, 0)\}$. Let us set

$$c_1 = \min_{\substack{(x,y)\in\mathbb{S}\\ x+y=1}} P_2(x, y), \tag{17}$$

We have, $c_1 > 0$ as it is the minumum of a positive continuous function on a compact set. In particular, for any $(x, y) \in \mathbb{S} \setminus \{0, 0\}$,

$$P_2(x, y) = (x + y)^2 P_2(x/(x + y), y/(x + y)) \geq c_1(x + y)^2. \tag{18}$$

For any nonnegative integer n, recall that we defined $\mathbb{S}(n)$ by (6). In particular, if P is a packing polynomial on $\mathbb{S}$, then $|\mathbb{S}(n) \cap \mathbb{Z}^2| = n$, see (7).

Lemma 5 *Let P, P_2 be defined by* (3) *and* (4). *Assume further that P_2 is positive on $\mathbb{S}\setminus\{(0, 0)\}$. Set c_1 as in* (17). *If*

$$n > \max\left\{\frac{8|a_{10}|^2}{c_1}, \frac{8|a_{01}|^2}{c_1}, 2|a_{00}|\right\}, \tag{19}$$

then for any $(x, y) \in \mathbb{S}(n)$ we have

$$x + y < \sqrt{\frac{2n}{c_1}}. \tag{20}$$

Proof Let n satisfy (19). We will show that, for any $(x, y) \in \mathbb{S}(n)$,

$$n > \frac{c_1}{2}(x + y)^2, \tag{21}$$

which is equivalent to the conclusion of the lemma. Using the definition of $\mathbb{S}(n)$ and (18) we have

$$\begin{aligned} n > P(x, y) &\geq P_2(x, y) - |a_{10}|x - |a_{01}|y - |a_{00}| \\ &\geq c_1(x + y)^2 - |a_{10}|x - |a_{01}|y - |a_{00}|. \end{aligned} \tag{22}$$

If $x + y \leq \max\{4|a_{10}|/c_1, 4|a_{01}|/c_1, 2\sqrt{|a_{00}|/c_1}\}$, then (21) follows from (19). Thus, we may assume that $x + y > 4|a_{10}|/c_1$, $x + y > 4|a_{01}|/c_1$, and $(x + y)^2 > 4|a_{00}|/c_1$. These inequalities together with (22) imply

$$\begin{aligned} n &> c_1(x + y)^2 \left(1 - \frac{|a_{10}|}{c_1(x + y)} \cdot \frac{x}{x + y} - \frac{|a_{01}|}{c_1(x + y)} \cdot \frac{y}{x + y} - \frac{|a_{00}|}{c_1(x + y)^2}\right) \\ &> c_1(x + y)^2 \left(1 - \frac{1}{4} \cdot \frac{x}{x + y} - \frac{1}{4} \cdot \frac{y}{x + y} - \frac{1}{4}\right) = \frac{c_1}{2}(x + y)^2. \end{aligned}$$

□

Proof (Proof of Theorem 2) We consider the sets $\mathbb{S}(n)$ as n increases and estimate the number of points $(x, y) \in \mathbb{S}(n)$ that satisfy (9).

For that purpose we start with some n, which is large enough. To be precise, we assume that n satisfies (19). Next we cover $\mathbb{S}(n)$ by squares and estimate the number of such squares. Namely, for any odd positive p and any real x and y let

$$\mathcal{Q}(x, y, p) = \{(u, v) \in \mathbb{R}^2 : x \leq u < x + p,\ y \leq v < y + p\}. \tag{23}$$

We consider squares of the form $\mathcal{Q}(px, py, p)$, where $p \in \mathbb{N}$ is a fixed odd number and x and y are non-negative integers. In particular, each such square contains p^2 integer points.

We point out that p is assumed to be odd, and so, the number of solutions $P(x, y) \equiv k \pmod{p}$ within each square is the same because $P(x + ap, y + bp) \equiv P(x, y) \pmod{p}$.

We say that $\mathcal{Q}(px, py, p)$ is *good* if all integer points in $\mathcal{Q}(px, py, p)$ are in $\mathbb{S}(n)$ and that it is *bad* if it has at least one integer point in $\mathbb{S}(n)$ and at least one integers point outside $\mathbb{S}(n)$. Our aim is to show that the proportion of bad squares becomes negligible as n tends to infinity. We have that $\mathcal{Q}(px, py, p)$ is bad if it belongs to one of the three families described below.

Case 1: at least one integer point in $\mathcal{Q}(px, py, p)$ lies below the line $y = \alpha x$. In particular, $\alpha \neq 0$ and the line $y = \alpha x$ intersects $\mathcal{Q}(px, py, p)$. Moreover, $(px + p, py)$ lies below the line $y = \alpha x$ and $(px, py + p)$ lies above the line. Therefore,

$$\alpha px < py + p, \qquad \alpha(px + p) > py.$$

Consequently,

$$\alpha x - 1 < y < \alpha x + \alpha,$$

So, for each x there are at most $\alpha + 2$ integer values of y.

Since $\mathcal{Q}(px, py, p) \cap \mathbb{S}(n) \cap \mathbb{Z}^2$ is non-empty, we have that for some integers $0 \leq u, v < p$

$$P(px + u, py + v) < n,$$

i.e., $(px + u, py + v) \in \mathbb{S}(n)$. Combining with Lemma 5, we have

$$x \leq x + y \leq \frac{px + u + py + v}{p} < \frac{1}{p}\sqrt{\frac{2}{c_1}}\sqrt{n}.$$

Setting

$$c_2 = \frac{1}{p}\sqrt{\frac{2}{c_1}} \tag{24}$$

we see that case 1 gives at most $(\alpha + 2)(c_2\sqrt{n} + 1)$ bad squares $\mathcal{Q}(px, py, p)$.

Case 2: at least one integer point in $\mathcal{Q}(px, py, p)$ lies above the line $x = \beta^{-1}y$. In particular, $\beta \neq \infty$ and the line $y = \beta x$ intersects $\mathcal{Q}(px, py, p)$. The analysis is completely analogous to case 1 and gives at most $(\beta + 2)(c_2\sqrt{n} + 1)$ bad squares.

Case 3: $\mathcal{Q}(px, py, p) \cap \mathbb{Z}^2 \subseteq \mathbb{S}$, but for some integers $0 \leq u_1, v_1, u_2, v_2 < p$,

$$P(px + u_1, py + v_1) < n \leq P(px + u_2, py + v_2).$$

In particular, $(px + u_1, py + v_1) \in \mathbb{S}(n)$. Since u_1, v_1, u_2, v_2 are bounded by p, we have for c_2 as above and for some positive c_3, c_4 depending only on p and the coefficients of P

$$\begin{aligned}
0 &< n - P(px + u_1, py + v_1) \leq P(px + u_2, py + v_2) - P(px + u_1, py + v_1)\\
&\leq |P_2(px + u_2, py + v_2) - P_2(px + u_1, py + v_1)|\\
&\quad + |P_1(px + u_2, py + v_2) - P_1(px + u_1, py + v_1)|\\
&\leq c_3(x + y) + c_4 \leq \frac{c_3}{p}(px + u_1 + py + v_1) + c_4\\
&< c_2c_3\sqrt{n} + c_4.
\end{aligned}$$

The last inequality comes from Lemma 5 and (24). Therefore, for sufficiently large n,

$$0 < n - P(px + u_1, py + v_1) < c_2c_3\sqrt{n} + c_4.$$

Since each bad square $Q(px, py, p)$ contains at least one such integer point $(px + u_1, py + v_1) \in \mathbb{S}(n)$ and P is injective on $\mathbb{S}_{\mathbb{Z}}$, case 3 gives us at most $c_2 c_3 \sqrt{n} + c_4$ exceptional squares.

Now we cover $\mathbb{S}(n)$ by squares $Q(px, py, p)$. Let $K(n)$ be the number of good squares, i.e., squares that satisfy $Q(px, py, p) \cap \mathbb{Z}^2 \subseteq \mathbb{S}(n)$. Since $|\mathbb{S}(n) \cap \mathbb{Z}^2| = n$ and the number of bad squares is $O(\sqrt{n})$, we conclude that $n = p^2 K(n) + O(\sqrt{n})$, where the constant in O-symbol depends on P, p, α, β but not on n.

Since P is a packing polynomial, the number of integer pairs $(u, v) \in \mathbb{S}(n)$ with

$$P(u, v) \equiv k \pmod{p} \tag{25}$$

is $\frac{n}{p} + \varepsilon$, where $|\varepsilon| \leq 1$. On the other hand, this amount is $K(n) \cdot N(p, k) + L(n)$, where $L(n)$ counts the number of $(u, v) \in \mathbb{S}(n)$ that satisfy (25), but lie in bad squares described by cases 1–3. In any case, $L(n) = O(\sqrt{n})$ and we conclude that $|N(p, k) - p| < cn^{-1/2}$ for all sufficiently large n. Since the left-hand side is independent of n, we have $N(p, k) = p$ for any odd p, as desired. □

7 Factorisation of P_2

.

We also need the following two lemmas:

Lemma 6 *For any odd prime p and for any integer j,* $0 \leq j \leq (p-1)/2$, *we have*

$$\frac{(p-1)!}{(j!)^2(p-1-2j)!} \equiv (-4)^j \binom{(p-1)/2}{j} \pmod{p}.$$

Proof Clearly, both sides equal 1 if $j = 0$. Now assume $j > 0$. Modulo p we have

$$\begin{aligned}\frac{(p-1)!}{(j!)^2(p-1-2j)!} &= \frac{(p-1)\cdots(p-2j)}{j!j!} \equiv \frac{(2j)!}{j!j!} = 2^j \frac{1}{j!}\prod_{i=0}^{j-1}(2i+1)\\ &\equiv (-2)^j \frac{1}{j!}\prod_{i=0}^{j-1}(p-1-2i) = (-2)^j 2^j \frac{1}{j!}\prod_{i=0}^{j-1}\left(\frac{p-1}{2} - i\right)\\ &= (-4)^j \binom{(p-1)/2}{j}.\end{aligned}$$

□

Lemma 7 *Let P be a quadratic polynomial of the form* (3) *that takes integer values on* $\mathbb{S}_{\mathbb{Z}}$. *For any odd prime p and any k,*

$$N(p, k) \equiv -(a_{11}^2 - 4a_{20}a_{02})^{(p-1)/2} \pmod{p}.$$

Proof Clearly,

$$1 - (P(x, y) - k)^{p-1} \equiv \begin{cases} 1 \pmod{p}, & \text{if } P(x, y) \equiv k \pmod{p},\\ 0 \pmod{p}, & \text{if } P(x, y) \not\equiv k \pmod{p}.\end{cases}$$

Thus, we have the following congruences modulo p:

$$
\begin{aligned}
N(p,k) &\equiv \sum_{x=0}^{p-1}\sum_{y=0}^{p-1}\left(1-(P(x,y)-k)^{p-1}\right)\\
&\equiv -\sum_{x=0}^{p-1}\sum_{y=0}^{p-1}(P(x,y)-k)^{p-1}\\
&\equiv -\sum_{x=0}^{p-1}\sum_{y=0}^{p-1}\sum_{j_1+\cdots+j_6=p-1}\frac{(p-1)!}{j_1!\cdots j_6!}\\
&\quad\times a_{20}^{j_1}a_{11}^{j_2}a_{02}^{j_3}a_{10}^{j_4}a_{01}^{j_5}(a_{00}-k)^{j_6}x^{2j_1+j_2+j_4}y^{j_2+2j_3+j_5}.
\end{aligned}
$$

On the other hand,

$$
\sum_{x=0}^{p-1}\sum_{y=0}^{p-1}x^iy^j \equiv \begin{cases}1 \pmod p, & \text{if } p-1 \mid i,\ p-1\mid j, \text{ and } i,j>0,\\ 0 \pmod p, & \text{otherwise.}\end{cases}
$$

Therefore, if we make summation by x and y first, the terms, where at least one of j_4, j_5, j_6 is positive, disappear. Hence,

$$
\begin{aligned}
N(p,k) &\equiv -\sum_{\substack{2j_1+j_2=p-1\\ j_2+2j_3=p-1}}\frac{(p-1)!}{j_1!j_2!j_3!}a_{20}^{j_1}a_{11}^{j_2}a_{02}^{j_3}\\
&= -\sum_{j=0}^{(p-1)/2}\frac{(p-1)!}{(j!)^2(p-1-2j)!}(a_{20}a_{02})^j a_{11}^{p-1-2j} \pmod p
\end{aligned}
$$

Combining this with Lemma 6, we obtain modulo p,

$$
N(p,k) \equiv -\sum_{j=0}^{(p-1)/2}(-4)^j\binom{(p-1)/2}{j}(a_{20}a_{02})^j a_{11}^{p-1-2j} = -(a_{11}^2-4a_{20}a_{02})^{(p-1)/2}.
$$

□

Theorem 3 *Let P be a quadratic packing polynomial on $\mathbb{S}$ and let D be defined by (11). We have $D=0$. In particular, up to a multiplicative constant, P_2 is the square of a linear polynomial.*

Proof By Theorem 2, $N(p,k)\equiv 0 \pmod p$ for odd p. Therefore, by Lemma 7, any odd prime p divides D. Hence $D=0$ and the claim follows. □

Corollary 4 *If P is a quadratic packing polynomial on $\mathbb{S}$, then*

$$
P_2(X,Y)=\frac{d}{2}(uX+vY)^2 \text{ for some } d,u,v\in\mathbb{Z}. \tag{26}
$$

Proof By Lemma 1, $2P_2(X,Y)\in\mathbb{Z}[X,Y]$. Now the claim follows from Theorem 3 and the Gauss Lemma. □

8 Density results

Let

$$
\mathbb{P}(n)=\{(x,y)\in\mathbb{S}: 0\le P_2(x,y)<n\}. \tag{27}
$$

Lemma 8 *If P is a packing quadratic polynomial on $\mathbb{S}_{\mathbb{Z}}$, then*

$$|\mathbb{S}(n) \cap \mathbb{Z}^2| - |\mathbb{P}(n) \cap \mathbb{Z}^2| = O(\sqrt{n}).$$

Proof The argument is very similar to what we did in case 3 in the proof of Theorem 2. The first term counts lattice points $(x, y) \in \mathbb{S}_{\mathbb{Z}}$ with $0 \leq P(x, y) < n$ while the second counts points with $0 \leq P_2(x, y) < n$. We estimate the size of the symmetric difference of both sets.

By Corollary 3, P_2 is positive on $\mathbb{S} \setminus \{(0, 0)\}$. Let c_1 be defined as in (17), $c_1 > 0$.

Case 1: $(x, y) \in \mathbb{P}(n)$, $(x, y) \notin \mathbb{S}(n)$, i.e.,

$$P_2(x, y) < n \leq P(x, y) = P_2(x, y) + a_{10}x + a_{01}y + a_{00}.$$

We have

$$x + y \leq c_1^{-1/2} P_2(x, y) < c_1^{-1/2} \sqrt{n}$$

and

$$\begin{aligned} 0 &\leq P(x, y) - n < P(x, y) - P_2(x, y) \\ &\leq \max\{|a_{10}|, |a_{01}|\}(x + y) + |a_{00}| \leq \max\{|a_{10}|, |a_{01}|\} c_1^{-1/2} \sqrt{n} + |a_{00}|. \end{aligned}$$

Since P is injective on $\mathbb{S}_{\mathbb{Z}}$, case 1 gives us at most $\max\{|a_{10}|, |a_{01}|\} c_1^{-1/2} \sqrt{n} + |a_{00}| + 1$ points (x, y).

Case 2: $(x, y) \in \mathbb{S}(n)$, $(x, y) \notin \mathbb{P}(n)$, i.e.,

$$P_2(x, y) + a_{10}x + a_{01}y + a_{00} = P(x, y) < n \leq P_2(x, y).$$

Without loss of generality we may assume that n is large enough, namely, that n satisfies (19).

$$\begin{aligned} 0 &< n - P(x, y) < P_2(x, y) - P(x, y) \\ &\leq \max\{|a_{10}|, |a_{01}|\}(x + y) + |a_{00}| \leq \max\{|a_{10}|, |a_{01}|\}(2c_1)^{-1/2} \sqrt{n} + |a_{00}|. \end{aligned}$$

The last inequality follows from Lemma 5. Since P is injective on $\mathbb{S}_{\mathbb{Z}}$, case 2 gives us at most $\max\{|a_{10}|, |a_{01}|\}(2c_1)^{-1/2} \sqrt{n} + |a_{00}|$ points (x, y) and the result follows. □

Lemma 9 *If P_2 is positive on $\mathbb{S} \setminus \{(0, 0)\}$, then*

$$|\mathbb{P}(n) \cap \mathbb{Z}^2| = \text{area}(\mathbb{P}(n)) + O(\sqrt{n}) = n \cdot \text{area}(\mathbb{P}(1)) + O(\sqrt{n}).$$

Proof This is same as Gauss's circle problem, except that instead of a circle, we have a homogeneous quadratic polynomial P_2. The proof is standard (see Lemma 2.1.1 of [6]), using unit squares to approximate the area covered by the region $\{(x, y) \in \mathbb{S} : P_2(x, y) < n\}$. In fact, cover the region by unit squares whose lower left corners lie inside the region. Then the number of unit squares protruding out of the region $\mathbb{P}(n)$ is proportional to the perimeter $\mathbb{P}(n)$, which is bounded from above by $c_5\sqrt{n} + c_6$ for some constants $c_5, c_6 > 0$ depending only on the coefficients of P_2 and α, β. □

Now combining Corollary 3, Lemmas 8 and 9 together with 7, we have the following result.

Corollary 5 *If P is a quadratic packing polynomial on $\mathbb{S}$, then* $\text{area}(\mathbb{P}(1)) = 1$.

9 Proof of the main result

Now, we prove the main theorem.

Proof of Theorem 1 By Corollary 4, $P_2(X,Y) = \frac{d}{2}(uX+vY)^2$ for some $d, u, v \in \mathbb{Z}$, $(u,v) \neq (0,0)$. In particular,

$$2a_{20} = du^2, \quad a_{11} = duv, \quad 2a_{02} = dv^2 \tag{28}$$

Clearly, $d > 0$ and $P_2(1,\alpha) \neq 0$, $P_2(\beta^{-1},1) \neq 0$ by Corollary 3. Without loss of generality we may assume that $\gcd(u,v) = 1$ and $u + \alpha v > 0$. By Corollary 3 again, $uX + vY$ does not change sign on $\mathbb{S} \setminus \{0,0\}$. Therefore, $\beta^{-1}u + v > 0$.

The set $\mathbb{P}(1)$ is the triangle bounded by the lines $y = \alpha x$, $x = \beta^{-1}y$ and $ux + vy = \sqrt{2/d}$. In particular, the vertices of the triangle are $(0,0)$ and

$$\left(\sqrt{\frac{2}{d}} \cdot \frac{1}{u+\alpha v}, \sqrt{\frac{2}{d}} \cdot \frac{\alpha}{u+\alpha v}\right), \left(\sqrt{\frac{2}{d}} \cdot \frac{\beta^{-1}}{\beta^{-1}u+v}, \sqrt{\frac{2}{d}} \cdot \frac{1}{\beta^{-1}u+v}\right).$$

Therefore, the area of $\mathbb{P}(1)$ is

$$\frac{1}{d}\begin{vmatrix} \frac{1}{u+\alpha v} & \frac{\alpha}{u+\alpha v} \\ \frac{\beta^{-1}}{\beta^{-1}u+v} & \frac{1}{\beta^{-1}u+v} \end{vmatrix} = \frac{1}{d} \cdot \frac{1-\alpha\beta^{-1}}{(u+\alpha v)(\beta^{-1}u+v)}.$$

Corollary 5 implies that

$$d(u+\alpha v)(\beta^{-1}u+v) = 1 - \alpha\beta^{-1}. \tag{29}$$

Combining with (28) we complete the proof. □

10 Stanton's result

Now consider the case, where $\alpha = 0$ and $\beta = n/m$ with $n, m \in \mathbb{N}$, $(m,n) = 1$. If P is a quadratic packing polynomial on $\mathbb{S}^{0,n/m}$, then after multiplication by n Eq. (8) becomes

$$2a_{20}m + a_{11}n = n. \tag{30}$$

Since the ray $\{(x,0) | x > 0\}$ lies in $\mathbb{S}^{0,n/m}$, Corollary 3 implies that $a_{20} > 0$. By Lemma 1, $2a_{20}$, $2a_{02}$ and a_{11} are integers.

Since $(n,m) = 1$, Eq. (30) implies that $n \mid (2a_{20})$. Write $2a_{20} = ns$ for some integer $s > 0$. Substituting into (30) and making cancellation we obtain $sm + a_{11} = 1$. In particular, $a_{11} \equiv 1 \pmod{s}$. On the other hand, Theorem 3 gives us

$$a_{11}^2 - (2a_{20})(2a_{02}) = 0. \tag{31}$$

Consequently, $a_{11}^2 \equiv 0 \pmod{s}$ since $s \mid (2a_{20})$. Therefore, $s = 1$ and $2a_{20} = n$, $a_{11} = 1 - m$. Now, Eq. (31) gives us $n \mid (m-1)^2$ and $2a_{02} = (m-1)^2/n$. Hence,

$$P_2(X,Y) = \frac{n}{2}\left(X + \frac{1-m}{n}Y\right)^2,$$

which is exactly Stanton's necessary condition.

Acknowledgements

The authors acknowledge SERB, DST, Government of India, for awarding us VJR/2017/000006 under the VAJRA Faculty Scheme which enabled the second author to visit the first author when this work was done. They are very grateful to a referee who pointed out a crucial correction to Theorem 2; it can be stated only for odd p, but this suffices. They also thank both the referees for other suggestions and for drawing attention to a recent reference. Data sharing not applicable to this article as no data sets were generated or analyzed during the current theoretical study.

Author details

[1]Statistics & Mathematics Unit, Indian Statistical Institute, 8th Mile Mysore Road, Bangalore 560059, India, [2]St. Petersburg Department of V. A. Steklov Institute of Mathematics, 27 Fontanka, St. Petersburg 191023, Russia.

Received: 9 April 2021 Accepted: 20 May 2022
Published online: 19 June 2022

References

1. Cantor, G.: Ein Beitrah Zur Mannigfaltigkeitslehre. J. Reine Angew. Math. **84**, 212–258 (1877)
2. Cantor, G.: Beiträge Zur Begrundung der Transfiniter Mengenlehre. Math. Ann. **46**, 484–512 (1895)
3. Chowla, P.: On some polynomials which represent every natural number exactly once. Det Kongelige Norske Widenskabers Selskabs Fordhandlinger **34**(Nr. 2), 8–9 (1961)
4. Fueter, R., Pólya, G.: Rationale Abzählung der Gitterpunkte. Vierteljschr. Naturforsch. Ges. Zürich **58**, 380–386 (1923)
5. Gjaldbæk, K. S.: Non-injectivity of nonzero discriminant polynomials and applications to packing polynomials. In: Nathanson M. B. (ed.), Combinatorial and Additive Number Theory IV, Springer Proceedings in Mathematics & Statistics, vol. 347, pp. 195–201 (2021)
6. Huxley, M.N.: Area, Lattice Points and Exponential Sums. London Mathematical Society Monographs, New Series, vol. 13. Oxford Science Publications, New York (1996)
7. Lew, J.S., Rosenberg, A.L.: Polynomial indexing of integer lattice points, I. J. Number Theory **10**, 192–214 (1978)
8. Lew, J.S., Rosenberg, A.L.: Polynomial indexing of integer lattice points, II. J. Number Theory **10**, 215–243 (1978)
9. Nathanson, M.B.: Cantor polynomials for semigroup sectors. J. Algebra Appl. **13**(5), 1350165 (2014)
10. Nathanson, M.B.: Cantor polynomials and the Fueter–Pólya theorem. Amer. Math. Monthly **123**(10), 1001–1012 (2016)
11. Smoryński, C.: Logical Number Theory I. An Introduction. Springer, New York (1991)
12. Stanton, C.: Packing polynomials on sectors of $\mathbb{R}^2$, Integers 14, Paper No. A, vol. 67, p. 13 (2014)
13. Vsemirnov, M. A.: Two elementary proofs of the Fueter–Pólya theorem on pairing polynomials, Algebra i Analiz, **13**(5), 1- -15 (2001). English translation: St. Petersburg Math. J., **13**(5), 705–715 (2002). Errata: Algebra i Analiz, **14**(5), 240 (2002). English translation: St. Petersburg Math. J., **14**(5), 887 (2003)

Publisher's Note