Groups generated by two bicyclic units in integral group rings

Eric Jespers
Dep. Mathematics
Vrije Universiteit Brussel
Pleinlaan 2
1050 Brussel, Belgium
efjesper@vub.ac.be

ngel del Ro
Dep. Matemáticas
Universidad de Murcia
Campus de Espinardo
30100 Murcia, Spain
adelrio@fcu.um.es

Manuel Ruiz
Dep. Mtodos Cuantitativos e Informticos
Universidad Politcnica de Cartagena
Paseo Alfonso XIII, 50
30.203 Cartagena, Spain
Manuel.Ruiz@upct.es

Proposed Running title: Groups generated by two bicyclics

Groups generated by two bicyclic units in integral group rings

Eric Jespers, ngel del Ro and Manuel Ruiz *

1 Introduction

In [5] Ritter and Sehgal introduced the following units, called the bicylic units, in the unit group $\mathcal{U}(\mathbb{Z}G)$ of the integral group ring $\mathbb{Z}G$ of a finite group G:

$$\beta_{a,g} = 1 + (1-g)a\widehat{g}, \quad \gamma_{a,g} = 1 + \widehat{g}a(1-g),$$

where $a, g \in G$ and $\widehat{g}$ is the sum of all the elements in the cyclic group $\langle g \rangle$.

It has been shown that these units generate a large part of the unit group of $\mathbb{Z}G$. Indeed, for most finite groups G, the bicyclic units together with the Bass cyclic units generate a subgroup of finite index in $\mathcal{U}(\mathbb{Z}G)$ [3, 6]. The Bass cyclic units are only needed to cover a subgroup of finite index in the centre and the group B generated by the bicyclic units contains a subgroup of finite index in a maximal $\mathbb{Z}$-order of each non-commutative simple image $M_n(D)$ of the rational group algebra $\mathbb{Q}G$. In particular, if $n > 1$, then B contains a subgroup of finite index in $\mathrm{SL}_n(\mathcal{O})$, where $\mathcal{O}$ is a maximal order in D; and hence B contains free subgroups of rank two. A next step in determining the structure of $\mathcal{U}(\mathbb{Z}G)$ is to investigate relations among the discovered generators. Presently this is beyond reach. Hence a more realistic goal is to study the structure of the group generated by two bicyclic units. In [4] Marciniak and Sehgal proved that if $\beta_{a,g}$ is a non trivial unit in $\mathbb{Z}G$ (here G is not necessarily finite) then the group $\langle \beta_{a,g}, \gamma_{a^{-1},g^{-1}} \rangle$ is free of rank 2. Clearly, bicyclic units are of the form $1 + a$ with $a^2 = 0$. Salwa, in [7], used the ideas of Marciniak and Sehgal to prove that if x and y are two elements of an additively torsion-free ring such that $x^2 = y^2 = 0$ and xy is not nilpotent then $\langle (1+x)^m, (1+y)^m \rangle$ is free of rank 2 for some positive integer m. In particular, if b_1 and b_2 are two bicyclic units and $(b_1 - 1)(b_2 - 1)$ is not nilpotent, then $\langle b_1^m, b_2^m \rangle$ is free of rank 2 for some positive integer m. In this paper we investigate the minimum positive integer m so that $\langle b_1^m, b_2^m \rangle$ is free provided that b_1 and b_2 are two bicyclic units so that $(b_1 - 1)(b_2 - 1)$ is not nilpotent. We prove the following theorem which indicates that if b_1 and b_2 are of the same type then frequently $m = 1$.

Theorem 1.1 *Let $b_1 = \beta_{x,g}$ and $b_2 = \beta_{y,h}$ be two bicyclic units of the same type in the dihedral group*

$$D_n = \langle a, b | a^n = b^2 = 1, ba = a^{-1}b \rangle$$

so that $\langle y, h \rangle \subseteq \langle x, g \rangle$. Then $\langle b_1, b_2 \rangle$ is either torsionfree abelian or free of rank 2.

As a consequence one obtains the following.

Corollary 1.2 *If p is prime and b_1 and b_2 are two bicyclic units of the same type of the dihedral group D_p then $\langle b_1, b_2 \rangle$ is either torsion free abelian or free of rank 2.*

*The first author has been partially supported by the Onderzoeksraad of Vrije Universiteit Brussel and the Fonds voor Wetenschappelijk Onderzoek (Vlaanderen) and the second by the D.G.I. of Spain and Fundacin Sneca of Murcia.

We prove Theorem 1.1 in Section 3. Before that we revisit Salwas's Theorem in Section 2 with the following two aims: first to present the tools needed in our proof of Theorem 1.1 and second to complement Salwa's result with the case that xy is nilpotent. Namely we prove the following

Theorem 1.3 *Let K be a subfield of $\mathbb{C}$ and R a finite dimensional K-algebra. Suppose a, b are two elements of R such that $a^2 = b^2 = 0$. The following properties hold:*

1. *if ab is nilpotent, then $\langle 1 + a, 1 + b\rangle$ is nilpotent;*
2. *if ab is not nilpotent then there is a positive integer m so that $\langle 1 + a, (1 + b)^m\rangle$ is free of rank 2.*

We finish the paper with some comments on the cases not included in Theorem 1.1. In particular we relate the problem for arbitrary dihedral groups to an open problem on free points for groups generated by a pair of 2×2-matrices (see for example the recent work of Bamberg [1]).

2 Nilpotent-Free dichotomy

In this section we prove Theorem 1.3. Many of the ideas are already in [7] where the second statement of the theorem is proved. Also, under some conditions (see the last part of Lemma 2.3) on a trace map, it is shown that $m = 1$. For completeness' sake we give a selfcontained proof.

Throughout this section K is a subfield of $\mathbb{C}$, R is a finite dimensional K-algebra and a and b are two elements of R so that $a^2 = b^2 = 0$. In order to prove Theorem 1.3 one may assume that $R = K[a, b]$. Let $J(R)$ denote the Jacobson radical of R. So $R/J(R) = \sum_{i=1}^{k} M_{n_i}(D_i)$, where D_i is a division K-algebra for every i.

If x is a real number then $\lfloor x\rfloor$ (resp. $\lceil x\rceil$) denotes the greatest (resp. smallest) integer not larger (resp. not smaller) than x.

Lemma 2.1 *For every $i = 1, \ldots, k$ one has $n_i \leq 2$ and D_i is a field. Furthermore, if $n_i = 1$ then $D_i = K$.*

Proof. Let $A = \mathbb{C}[a, b] = \mathbb{C} \otimes_K K[a, b] = \mathbb{C} \otimes_K R$. First we prove that every simple quotient of $A/J(A)$ is of the form $M_m(\mathbb{C})$ with $m \leq 2$. We may assume without loss of generality that A is simple, so that $A = M_m(\mathbb{C})$ for some positive integer m and we identify A with the endomorphism ring of an m-dimensional complex vector space. Let $B = \mathbb{C}[ab]$. Then $A = B + Ba + bB + bBa$ and hence $\dim_{\mathbb{C}} A \leq 4 \dim_{\mathbb{C}} B$. Since $a^2 = 0$ we have $\operatorname{Im} a \subseteq \operatorname{Ker} a$ and hence $2 \dim_{\mathbb{C}} \operatorname{Im} a \leq m$. Consequently, $\dim_{\mathbb{C}} \operatorname{Im} ab \leq \dim_{\mathbb{C}} \operatorname{Im} a \leq \left\lfloor \frac{m}{2} \right\rfloor$. The Cayley-Hamilton Theorem then implies that ab satisfies a polynomial identity of degree at most $\left\lfloor \frac{m}{2} \right\rfloor + 1$. Hence $\dim_{\mathbb{C}} B \leq \left\lfloor \frac{m}{2} \right\rfloor + 1$ and thus $m^2 = \dim_{\mathbb{C}} A \leq 4(\left\lfloor \frac{m}{2} \right\rfloor + 1)$. Consequently $\left(\frac{m}{2}\right)^2 \leq \left\lfloor \frac{m}{2} \right\rfloor + 1$, and therefore $m \leq 2$.

Clearly, both $J(R)$ and $J(A)$ are nilpotent. As A is a central extension of R we know that $J(R) = J(A) \cap R$. So we consider $R/J(R)$ as a subring of $A/J(A)$.

Let $S = M_n(D)$, with D a division ring, be a simple quotient of R. By the above S is embedded in a simple quotient $M_m(\mathbb{C})$ of A, with $m \leq 2$. Hence every complete set of orthogonal idempotents of S has at most 2 elements. So $n \leq 2$. Furthermore, if $n = 2$, then $m = 2$ and D being the double centralizer of a set of a primitive idempotents yields that $D \subseteq \mathbb{C}$. So, in this case, D is a field. On the other hand, if $m = 1$, then the natural images $\overline{a}$ and $\overline{b}$ in $S = D$ are zero. Hence $S = K\left[\overline{a}, \overline{b}\right] = K$. This proves the result. ∎

Lemma 2.2 *Let $A = M_2(D)$ where D is a division ring and $a, b \in A$ so that $a^2 = b^2 = 0$. If ab is nilpotent then $ab = ba = 0$.*

Proof. Again, we identify A with the endomorphism ring of a two dimensional vector space V over D. If $ab \neq 0$ then Ker ab = Ker b = Im b and Im ab = Im a = Ker a. Let $0 \neq v_1 \in$ Im a and $v_2 \in V$ so that $a(v_2) = v_1$. Then $V = \langle v_1, v_2 \rangle$. Furthermore $(ab)(v_1) = \lambda v_1$ for some $\lambda \in K$. Since ab is nilpotent, $\lambda = 0$. Thus $(ab)^2 = 0$ and therefore Ker b = Ker ab = Im ab = Im a. We conclude that $ab = 0$, a contradiction. ∎

Lemma 2.2 implies that if ab is nilpotent, then $Ra + J(R)$ and $Rb + J(R)$ are nilpotent left ideals of R. So $a, b \in J(R)$. Hence $\langle 1+a, 1+b \rangle$ is contained in the (multiplicative) nilpotent group $1 + J(R)$. This proves statement 1 of Theorem 1.3.

To prove the second statement of Theorem 1.1, first recall that from from Sanov's Theorem [8] and a change of basis argument it is easy to deduce that if z and w are two complex numbers so that $|zw| \geq 4$, then the following two matrices generate a free group of rank 2:

$$\begin{pmatrix} 1 & z \\ 0 & 1 \end{pmatrix}, \quad \begin{pmatrix} 1 & 0 \\ w & 1 \end{pmatrix}$$

If ab is not nilpotent, then $\rho(ab)$ is not nilpotent where $\rho : R \to M_{n_i}(D_i)$ is an epimorphism for some $i = 1, \ldots, k$ with $n_i = 2$. Statement 2 of Theorem 1.3 then follows from the following Lemma.

Lemma 2.3 *Let $A = M_2(K)$, where K is a subfield of $\mathbb{C}$ and $a, b \in A$ so that $a^2 = b^2 = 0$ and ab is not nilpotent. Then $\langle 1 + a, 1 + mb \rangle$ is a free group for some positive integer m. If, moreover, $|tr(ab)| \geq 4$, then $\langle 1 + a, 1 + b \rangle$ is a free group.*

Proof. Again we identify A with the endomorphism ring of the two dimensional K-vector space K^2. Since ab is not nilpotent of rank 1, after a change of basis in K^2 one may assume that

$$ab = \begin{pmatrix} \lambda & 0 \\ 0 & 0 \end{pmatrix}$$

for some nonzero $\lambda \in K$.Hence, as Im a = Im ab and Ker b = Ker ab one has that

$$a = \begin{pmatrix} p & r \\ 0 & 0 \end{pmatrix} \quad \text{and} \quad b = \begin{pmatrix} q & 0 \\ s & 0 \end{pmatrix}$$

for some $p, q, r, s \in K$. Because a and b are nonzero nilpotent elements, $p = 0 = q$ and $r \neq 0$ and $s \neq 0$. Thus

$$1 + a = \begin{pmatrix} 1 & r \\ 0 & 1 \end{pmatrix} \quad \text{and} \quad 1 + b = \begin{pmatrix} 1 & 0 \\ s & 1 \end{pmatrix}.$$

By Sanov's Theorem $\langle 1 + a, 1 + mb \rangle$ is a free group for $m = \left\lceil \frac{4}{|rs|} \right\rceil$. If $|tr(ab)| \geq 4$, then $|rs| \geq 4$ and hence $m = 1$. ∎

Proposition 2.4 *Let A be a $\mathbb{Q}$-algebra which is a direct product of division rings and 2×2-matrix rings over subfields of $\mathbb{C}$. Suppose $a, b \in A$ are such that $a^2 = b^2 = 0$. The following properties hold:*

1. *if ab is nilpotent, then $\langle 1 + a, 1 + b \rangle$ is torsionfree abelian;*

2. *if ab is not nilpotent, then there exists an integer m so that $\langle 1+a, 1+mb\rangle$ is free of rank 2. Moreover if $|\mathrm{tr}(\rho(ab))| \geq 4$, for some projection $\rho : A \to M_2(K)$ onto a simple quotient of A, then $\langle 1+a, 1+b\rangle$ is free of rank 2.*

Proof. Everything is an immediate consequence of Lemma 2.2 and Lemma 2.3 except the torsion-freeness of the abelian case.

Assume that $u = (1+a)^k(1+b)^l$ is a periodic element of order m in the abelian group $\langle 1+a, 1+b\rangle$ (with $k, l \in \mathbb{Z}$). Then, $1+kma = 1-lmb$ and so $ka = -lb$. Hence, $(1+a)^k = 1+ka = 1-lb = (1+b)^{-l}$ and thus $u = 1$. ∎

3 Bicyclic units

In this section we prove Theorem 1.1. Let $b_1 = \beta_{x,g}$ and $b_2 = \beta_{y,h}$ be two bicyclic units of D_n so that $\langle y, h\rangle \subseteq \langle x, g\rangle$. Note that $\mathbb{Q}D_n$ satisfies the conditions of Proposition 2.4. So either $\langle b_1, b_2\rangle$ is torsionfree abelian or $\langle b_1, b_2^k\rangle$ is free of rank 2 for some $k \geq 1$. We have to prove that in the former case one can take $k = 1$. For that we make use once more of Proposition 2.4 and we only have to prove that if b_1 and b_2 do not commute then there exists an irreducible complex character χ of degree 2 of D_n so that $|\chi(\alpha)| \geq 4$, where $\alpha = (b_1 - 1)(b_2 - 1)$.

So in the remainder we assume that b_1 and b_2 do not commute. This imply that both g and h do not belong to $\langle a\rangle$ and hence $\langle x, g\rangle$ is a dihedral group. Therefore one may assume without loss of generality that $D_n = \langle x, g\rangle$. Since $\beta_{a^ib,a^jb} = \beta_{a^{i-j},a^jb}$, without loss of generality, we may assume that $D_n = \langle x, g\rangle$, $x, y \in \langle a\rangle$ and changing generators if necessary, $x = a$ and $g = b$. Summarizing $b_1 = \beta_{a,b}$ and $b_2 = \beta_{a^i,a^jb}$ for some $1 \leq i, j < n$ and $2i \neq n$.

The non-linear irreducible complex characters of D_n are all maps χ_k, with $1 \leq k < \frac{n}{2}$, given by

$$\chi_k(a^t) = \xi^t + \xi^{-t}, \quad \chi_k(a^tb) = 0$$

for every $0 \leq t < n$, where ξ denotes an n-th root of unity.

For every $m \in \mathbb{Z}$ we denote:

$$\eta_m = \xi^m + \xi^{-m} = 2\cos\frac{2\pi m}{n}, \quad \nu_m = \xi^m - \xi^{-m} = 2\sin\frac{2\pi m}{n}.$$

The following formulae are easily verified:

$$\begin{aligned} \eta_n\eta_m &= \eta_{n+m} + \eta_{n-m} \\ \nu_n\nu_m &= \eta_{n+m} - \eta_{n-m} \\ \nu_m\eta_n &= \nu_{m+n} + \nu_{m-n}. \end{aligned}$$

Then

$$\begin{aligned} \alpha = {} & a^{i+1} - a^{i-1} + a^{-i-1} - a^{1-i} + a^{1-i-j} + a^{i-1-j} - a^{1+i-j} - a^{-1-i-j} + \\ & (a^{1-i} + a^{i-1} - a^{1+i} - a^{-1-i} + a^{1+i+j} + a^{-1-i+j} - a^{-1+i+j} - a^{1-i+j})b \end{aligned}$$

and hence

$$\begin{aligned} \chi_k(\alpha) &= \eta_{(i+1)k} - \eta_{(i-1)k} + \eta_{(-1-i)k} - \eta_{(1-i)k} + \eta_{(1-i-j)k} + \eta_{(i-1-j)k} - \eta_{(1+i-j)k} - \eta_{(-1-i-j)k} \\ &= 2\nu_k\nu_{ik} + \eta_{-jk}(\nu_{(1-i)k} - \nu_{(1+i)k}) = \nu_k\nu_{ik}(2 - \eta_{jk}) \\ &= 8\sin\tfrac{2\pi k}{n}\sin\tfrac{2\pi ik}{n}(1 - \cos\tfrac{2\pi jk}{n}) = 16\sin\tfrac{2\pi k}{n}\sin\tfrac{2\pi ik}{n}\sin^2\tfrac{\pi jk}{n}. \end{aligned}$$

The existence of a character with the required properties then follows from the following Lemma. The remainder of the section is devoted to its proof. Unfortunately the proof is longer than one would like. On the other hand the remarks given in Section 4 indicates that the inequality of the Lemma is quite elusive.

Lemma 3.1 *If i, j, n are positive integers such that $1 \le i, j < n$, $n \ge 3$ and $(n, i, j) \ne (6, 3, 1)$ then there is $k \in \mathbb{Z}$ such that*

$$\left|\sin \frac{2\pi k}{n} \ \sin \frac{\pi i k}{n} \ \sin^2 \frac{\pi j k}{n}\right| \ge \frac{1}{4}. \tag{3.1}$$

Proof. For every integer $a \in \mathbb{R}$ let $s_a = \frac{2\pi a}{n}$ and $f_a : \mathbb{R} \to \mathbb{R}/2\pi\mathbb{Z} = S$ be the map defined by $f_a(x) = s_a x + 2\pi\mathbb{Z}$.

Let i, j, n be integers satisfying the conditions of the Lemma. Without loss of generality we may assume that $i, j \le \frac{n}{2}$, so that $s_i, s_j \le \pi$. Let $f = f_{i,j} : [0, n) \to T = S^2$ be defined by $f(x) = (f_i(x), f_j(x))$. The image of f is a spiral on the torus T.

We identify S with $[0, 2\pi)$ and T with the square $[0, 2\pi)^2$, so that we consider f_a as a map $\mathbb{R} \to [0, 2\pi)$. Let D denote the diagonal of T and $V = \left[\frac{\pi}{2}, \frac{3\pi}{2}\right]^2$.

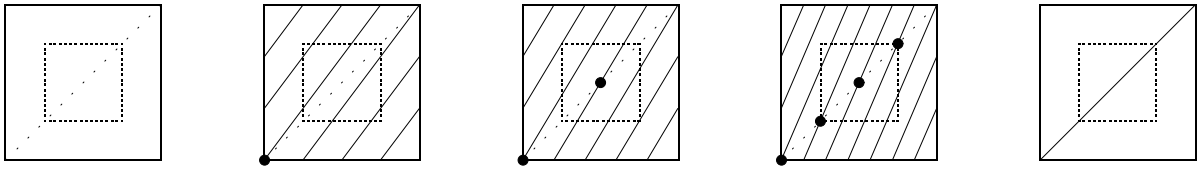

Figure 1

The first of the pictures in Figure 1 represents T (the big square), D (the dotted line) and V (the small square). The other pictures include the image of f for different values of j/i.

Let

$$W = \left[\frac{n}{8}, \frac{3n}{8}\right], \quad W_1 = \left[\left\lceil \frac{n}{8} \right\rceil, \left\lfloor \frac{3n}{8} \right\rfloor\right], \quad X = f^{-1}(D)$$

and consider the following four conditions:

(1) There are $k_1, k_2 \in \mathbb{Z}$ such that $\left|\sin f_i(k_1) \sin f_i(k_1/2) \sin^2 f_j(k_1/2)\right| \ge \frac{1}{4}$ and $\left|\sin f_i(k_1) \sin^2 f_i(k_1/2) \sin f_j(k_1/2)\right| \ge \frac{1}{4}$.

(2) There are $k_1, k_2 \in \mathbb{Z} \cap W$ such that $\left|\sin f_i(k_1/2) \sin^2 f_j(k_1/2)\right| \ge \frac{\sqrt{2}}{4}$ and $\left|\sin^2 f_i(k_2/2) \sin f_j(k_2/2)\right| \ge \frac{\sqrt{2}}{4}$.

(3) $f(\mathbb{Z} \cap W) \cap V \ne \emptyset$.

(4) $f(W_1) \cap D \cap V \ne \emptyset$.

Condition (1) is equivalent to the statement of the lemma. This condition is introduced to get symmetry in the roles of i and j. Clearly (3) implies (2) and (2) implies (1). Now we prove that (4) implies (3). Let $t \in W_1$ be such that $f(t) \in V \cap D$. Then there is an integer l such that $l \le t \le l + 1$ and $l, l + 1 \in W_1 \subseteq W$. Assume that $i \le j$. Since $s_j \le \pi$ and $\frac{\pi}{2} \le f_j(t) \le \frac{3\pi}{2}$, then either $\frac{\pi}{2} \le f_j(l) \le f_i(l) \le f_i(t) \le \frac{3\pi}{2}$ or $\frac{\pi}{2} \le f_i(t) \le f_i(l + 1) \le f_j(l + 1) \le \frac{3\pi}{2}$. Thus (3) holds.

We now argue by contradiction. So assume the Lemma is not true and thus that the conditions (1) to (4) do not hold. Hence, from now on we work under the following assumptions:

(C1) either, for every $k \in \mathbb{Z}$, $\left|\sin f_1(k) \sin f_i(k/2) \sin^2 f_j(k/2)\right| < \frac{1}{4}$, or, for every $k \in \mathbb{Z}$, $\left|\sin f_1(k) \sin^2 f_i(k/2) \sin f_j(k/2)\right| < \frac{1}{4}$.

(C2) either for every $k \in \mathbb{Z}$, $\left|\sin f_i(k/2) \sin^2 f_j(k/2)\right| < \frac{\sqrt{2}}{4}$, or for every $k \in \mathbb{Z}$, $\left|\sin^2 f_i(k/2) \sin f_j(k/2)\right| < \frac{\sqrt{2}}{4}$.

(C3) $f(\mathbb{Z} \cap W) \cap V = \emptyset$.

(C4) $f(W_1) \cap D \cap V = \emptyset$ or equivalently $W_1 \cap X \cap f^{-1}(V) \neq \emptyset$.

An exhaustive computer search shows that the only triple of positive integers (n, i, j) with $n \leq 200$ and $i, j \leq \frac{n}{2}$ for which there is not an integer k satisfying (3.1) is $(n, i, j) = (6, 3, 1)$; precisely the case excluded in the statement of the Lemma. So we assume $n > 200$. Note that because of condition (C4) and the fact that $s_i, s_j \leq \pi$ we also easily deduce that $i \neq j$. Moreover, because of the symmetry of the roles of i and j, we may also assume that $i < j$.

We introduce the following notation:

$$\begin{aligned} m &= \gcd(i, j) = |f^{-1}(0, 0)| \\ v &= \frac{j - i}{m} = |D \cap \text{ Im } f| \\ \alpha &= \frac{n}{mv} \\ \theta &= f_i(\alpha) (= f_j(\alpha)). \end{aligned}$$

Then

$$\begin{aligned} X &= \{k\alpha : k = 0, 1, \ldots, mv - 1\} \text{ and} \\ f(X) &= D \cap \text{Im } f = \{(\frac{2\pi k}{v}, \frac{2\pi k}{v}) : k = 0, 1, \ldots, v - 1\} \end{aligned}$$

It is clear that $f(X)$ is a cyclic subgroup of $D \cap T$ of order v and (θ, θ) is a generator of $f(X)$. The dots in the previous picture represent the elements of $f(X)$.

Since $f(X) \cap V = \text{Im } f \cap V \cap D$, condition (C4) implies that

(C5) If I is an interval so that $f(I) = \text{Im } f$ then $f(X) \cap V \subseteq f((I \setminus W_1) \cap X)$.

Since $\alpha = \frac{n}{j-i} > 2$, every interval of length ≤ 2 contains at most one element of X and therefore condition (C4) implies

$$\left|\left[\frac{n}{8}, \left\lceil\frac{n}{8}\right\rceil\right] \cap X\right| \leq 1, \quad \left|\left[\left\lfloor\frac{3n}{8}\right\rfloor, \frac{3n}{8}\right] \cap X\right| \leq 1 \quad \text{and hence} \quad \left|W \cap X \cap f^{-1}(V)\right| \leq 2. \tag{3.2}$$

We consider separately the mutually exclusive cases (1) $v \neq 1$ and $mv \neq 2$, (2) and $v = 1$ and $m \geq 3$ and (3) $mv \leq 2$.

Case 1: $v \neq 1$ and $mv \neq 2$. First we show that $m \leq 4$. Note that

$$|f(X) \cap V| = \begin{cases} \frac{v}{2} + 1 & \text{if} \quad v \equiv 0 \mod 4 \\ \frac{v}{2} & \text{if} \quad v \equiv 2 \mod 4 \\ \frac{v+1}{2} & \text{if} \quad v \equiv 3 \mod 4 \\ \frac{v-1}{2} & \text{if} \quad v \equiv 1 \mod 4 \end{cases} \tag{3.3}$$

which is different from 0. Let I be the interval centred at $\frac{n}{4}$ and of length $\frac{n}{m}$. As $f(I) = \text{Im } f$, condition (C5) implies that I is not contained in W_1 and this implies that $m \leq 4$.

Second we show that $m \neq 4$. So, suppose the contrary, that is assume $v \neq 1$ and $m = 4$. Because W has length $\frac{n}{m} = \frac{n}{4}$, we get that $f(W) = \text{Im } f$ and by (C5) we have $f(X) \cap V \subseteq f((W \setminus W_1) \cap X)$.

So that $|f(X) \cap V| \leq 2$, by (3.2). As, by assumption, $v \neq 1$, we obtain easily from (3.3) that either $v = 2, 3$ or $v = 5$. However if $v = 3$ or $v = 5$ then $X \cap W = \{\frac{2n}{12}, \frac{3n}{12}, \frac{4n}{12}\}$ or $X \cap W = \{\frac{3n}{20}, \frac{4n}{20}, \frac{5n}{20}, \frac{6n}{20}, \frac{7n}{20}\}$ respectively, so that $X \cap W \subseteq W_1$ and thus $f(X) \cap V = \emptyset$, a contradiction. So $v = 2$ and hence $f(\frac{n}{8}) = (\pi, \pi) = f(\frac{3n}{8})$. By condition (C3) n is not a multiple of 8. Because of (C3) we know that $f(\lceil \frac{n}{8} \rceil) \notin V$ and so $f_j(\lceil \frac{n}{8} \rceil) > \frac{3\pi}{2}$. Thus

$$\frac{\pi}{2} < f_j(\left\lceil \frac{n}{8} \right\rceil) - f_j(\frac{n}{8}) = s_j\left(\lceil n/8 \rceil - n/8\right) \leq \pi\left(\left\lceil \frac{n}{8} \right\rceil - \frac{n}{8}\right)$$

and hence $n \equiv q \mod 8$ with $q = 1, 2$ or 3. This implies that for $k = \lfloor \frac{n}{8} \rfloor$ one has

$$\frac{5\pi}{8} \leq \pi - \frac{q\pi}{8} = f_j(k) < f_i(k) < \pi$$

and

$$\frac{\pi}{4} > f_1(k) = \frac{2\pi\frac{n-q}{8}}{n} = \frac{\pi}{4} - \frac{\pi q}{4n} \geq \frac{\pi}{4} - \frac{3\pi}{800} = \frac{197\pi}{800}.$$

Consequently,

$$\left|\sin f_1(k)\ \sin\frac{f_i(k)}{2}\ \sin^2\frac{f_j(k)}{2}\right| \geq \sin\frac{197\pi}{800}\ \sin^3\frac{5\pi}{8} \geq \frac{1}{4}$$

and

$$\left|\sin f_1(k)\ \sin^2\frac{f_i(k)}{2}\ \sin\frac{f_j(k)}{2}\right| \geq \sin\frac{197\pi}{800}\ \sin^3\frac{5\pi}{8} \geq \frac{1}{4}$$

in contradiction with (C1).

Third we show $m \neq 3$. Suppose the contrary, that is, assume $m = 3$. Let $I = \left[0, \frac{n}{3}\right]$. Then $f(X) \cap V \subseteq f(\left[0, \lceil \frac{n}{8} \rceil\right] \cap X)$, by (C5). Note that $\left[0, \frac{n}{8}\right] \cap X = \{\frac{kn}{3v} \mid 1 \leq k \leq \frac{3v}{8}\}$ has $\lfloor \frac{3v}{8} \rfloor$ elements. So (3.2) implies

$$|f(X) \cap V| \leq |X \cap (0, \left\lceil \frac{n}{8} \right\rceil)| \quad \leq \quad \left\lfloor \frac{3v}{8} \right\rfloor + 1 \tag{3.4}$$

Hence a careful analysis of inequality (3.4) and (3.3) yields that $v = 9, 2, 3, 5$ or 6 and in all these cases $|f(X) \cap V| > \lfloor \frac{3v}{8} \rfloor$. We conclude that $X \cap \left[\frac{n}{8}, \lceil \frac{n}{8} \rceil\right]$ has one element. The latter is $\frac{4n}{27}$ if $v = 9$, $\frac{n}{6}$ if $v = 2$, $\frac{2n}{9}$ if $v = 3$, $\frac{2n}{15}$ if $v = 5$, and $\frac{3n}{18}$ if $v = 6$. The smallest of the listed numbers is $\frac{2n}{15}$ and thus we get

$$\frac{n}{8} \leq \frac{2n}{15} \leq \left\lceil \frac{n}{8} \right\rceil.$$

Consequently $\frac{n}{120} = \frac{2n}{15} - \frac{n}{8} < 1$. So $n < 120$, and this contradicts the assumption that $n > 200$.

We conclude that $m \leq 2$. Note that it follows that $f(\frac{n}{4}) \neq (0, 0)$. We claim that mv is not a multiple of 4 for otherwise $f(\frac{n}{4}) \in f(W_1) \cap V \cap D$; in contradiction with (C4).

Consider the maps $g : [0, n) \to \mathbb{R}$ and $\bar{g} : [0, n) \to T$ given by $g(t) = \frac{\theta}{\alpha}t$ and $\bar{g}(t) = (g(t) + 2\pi\mathbb{Z}, g(t) + 2\pi\mathbb{Z})$. So the image of $\bar{g}$ is D and $\bar{g}(t) = f(t)$ for every $t \in X$. Because of condition (C4), one has

$$\bar{g}(X \cap W_1) \cap V = \emptyset. \tag{3.5}$$

Assume now that $\frac{\pi}{2} < \theta < \frac{3\pi}{2}$. Then, by condition (C4), $\alpha = \frac{n}{mv} \notin W_1$ and because $mv > 2$, $\alpha < \lceil \frac{n}{8} \rceil$. Because 4 does not divide mv we get that $mv \geq 9$. The restriction on θ easily yields that if $W_1 \cap X$ has at least three elements then $W_1 \cap X \cap f^{-1}(V) \neq \emptyset$, contradicting (C4). Thus we get $|W_1 \cap X| \leq 2$. Hence the length of the interval W_1 is at most 2α and at least $\frac{n}{4} - 2$. Therefore $\frac{2n}{9} \geq 2\alpha \geq \frac{n}{4} - 2$ and this implies that $n \leq 72$, a contradiction.

So it remains to deal with the situation $\theta \leq \frac{\pi}{2}$ or $\theta \geq \frac{3\pi}{2}$. We deal with $\theta \leq \frac{\pi}{2}$ (the other case is dealt with similarly). Clearly then $v \geq 4$. Because 4 does not divide mv it follows that $v \geq 5$ and $v \neq 8$. If $v = 6$, then $\frac{n}{3} \in W_1 \cap X$ and $\bar{g}(\frac{n}{3}) \in V$; if $v = 7$ and $m = 1$ then $\frac{2n}{7} \in W_1 \cap X$ and $\bar{g}(\frac{2n}{7}) \in V$; and if $v = 7$ and $m = 2$ then $\frac{n}{7} \in W_1 \cap X$ and $\bar{g}(\frac{n}{7}) \in V$. These three cases yields to a contradiction with (3.5) so that $v = 5$ or $v \geq 9$.

Assume first that $v = 5$. If $m = 2$, then $2\alpha = \frac{n}{5} \in W_1 \cap X$ and $\bar{g}(2\alpha) \in V$, again a contradiction with (3.5). Thus $m = 1$ and $g(\alpha) = \frac{2\pi}{5}$. Because of (C3) one has $f(\mathbb{Z} \cap I) \cap V = \emptyset$, where $I = \left[\frac{n}{5}, \frac{n}{4}\right]$. Moreover, for every $x \in I$, $f_i(x) \leq f_j(x) \leq f_i(x) + \frac{\pi}{2}$, that is $f(I)$ is in the strip between the diagonal and the parallel of the diagonal through $A = (\frac{\pi}{2}, \pi)$. (Note that this last has a continuation in the lower right corner as it is shown in Figure 2.)

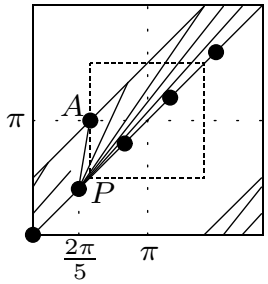

Figure 2

The dots on the diagonal represent the elements of $f(X)$, $f(\alpha) = (\frac{2\pi}{5}, \frac{2\pi}{5})$ is labelled by P. The lines leaving P represent several possibilities for $f(I)$. All of them leave in P and end in the line parallel to the diagonal through A. The length of the interval $f_i(I)$ is at least $\frac{\pi}{10}$, and the equality holds if and only if $i = 1$. If $i = 1$ then $f\left(\frac{n}{4}\right) = A$ and $f(I)$ is the segment joining P and A. Then $f\left(\left\lceil \frac{n}{4} \right\rceil\right) \in V$ contradicting (C3). Therefore $i \neq 1$ and hence $f(I)$ intersects the interior of V and in fact $f\left[\frac{n}{5}, \frac{9n}{40}\right]$ intersects V. This is because the length of $f_i\left[\frac{n}{5}, \frac{9n}{40}\right]$ is $\frac{\pi i}{20} \geq \frac{\pi}{10}$, and hence there exists $t \in \left[\frac{n}{5}, \frac{9n}{40}\right]$ with $f_i(t) = f_i\left(\frac{n}{5}\right) + \frac{\pi}{10} = \frac{\pi}{2}$ and for such a t one has $f(t) \in V$ (look at the picture). Let t be the smallest element of I so that $f(t) \in V$ and set $k = \lfloor t \rfloor$. Then $k + 1 \in I$ and hence $f(k+1) \notin V$. This implies that $f_i(k+1) > \pi$ (look at Figure 2) and therefore $\frac{\pi}{2} < f_i(k+1) - f_i(k)$, so that the slope of f_i is larger than $\frac{\pi}{2}$. Thus

$$\frac{\pi}{2} = \frac{2\pi}{5} + \frac{\pi}{10} \leq f_i(\lfloor \alpha \rfloor + 1) \leq f_j(\lfloor \alpha \rfloor + 1) \leq \frac{3\pi}{2}$$

so that $f(\lfloor \alpha \rfloor + 1) \in V$, a contradiction with (C3).

Finally, assume that $v \geq 9$ and recall that we are assuming $\theta \leq \frac{\pi}{2}$. Let l be the first non negative integer such that $g(l\alpha) \geq \pi/2$ and p the least positive integer such that $g((l+p)\alpha) > 3\pi/2$. Note that the first inequality implies that $(l-1)\alpha < \frac{n}{4}$. Since $\alpha \leq \frac{n}{9}$ we thus get that $l\alpha \leq \frac{n}{3} < \left\lfloor \frac{3n}{8} \right\rfloor$ (recall that $n > 200$). Since $\theta \leq \pi/2$, we have that $l, p \geq 2$. We claim that $p = 2$. Assume that $p \geq 3$. Let $\beta = (l + p - 1)\alpha$. Then $\overline{g}(\beta) \in V$ and because of condition (3.5), $\beta \notin W_1$. As also, by assumption, $p \geq 3$ and because $g((l+p)\alpha) > \frac{3\pi}{2}$ it thus follows that $g(\beta) > \frac{3\pi}{2} - \frac{\pi}{3} = \frac{7\pi}{6}$. So that the length of $g[0, \beta]$ is at least $\frac{7\pi}{6}$. If $\beta \leq \left\lceil \frac{n}{8} \right\rceil$, then the length of $g(W_1)$ is at least

$$\frac{7\pi}{6} \frac{\left\lfloor \frac{3n}{8} \right\rfloor - \left\lceil \frac{n}{8} \right\rceil}{\left\lceil \frac{n}{8} \right\rceil} \geq \frac{7\pi}{3} \frac{n-6}{n+7} \geq 2\pi.$$

This implies that $\bar{g}(W_1 \cap X) \cap V \neq \emptyset$, contradicting (3.5). So $\beta > \left\lceil \frac{n}{8} \right\rceil$ and hence, as $\beta \notin W_1$, we also get $\beta > \left\lfloor \frac{3n}{8} \right\rfloor$. Let k be the greatest non negative integer such that $(l+k)\alpha \leq \left\lfloor \frac{3n}{8} \right\rfloor$ (recall

that $l\alpha < \left\lfloor \frac{3n}{8} \right\rfloor$). Thus $k < p-1$. As $f((l+k)\alpha) \in V$ and thus $(l+k)\alpha \notin W_1$, we obtain that $(l+k)\alpha < \left\lceil \frac{n}{8} \right\rceil$. Consequently,

$$\left\lfloor \frac{3n}{8} \right\rfloor < (l+k+1)\alpha \leq 2(l+k)\alpha \leq 2\left\lceil \frac{n}{8} \right\rceil \leq \frac{n+7}{4} \leq \left\lfloor \frac{3n}{8} \right\rfloor$$

a contradiction. So indeed $p = 2$. Consequently, $\frac{\pi}{2} + 3\theta > \frac{3\pi}{2}$ and thus $\theta > \frac{\pi}{3}$. Hence, $g(2\alpha) > \frac{2\pi}{3} > \frac{\pi}{2}$. Thus $l = 2$ and so $\bar{g}(3\alpha) \in V$, so that $3\alpha \notin W_1$. Since $3\alpha \leq \frac{n}{3}$ we get $3\alpha < \left\lceil \frac{n}{8} \right\rceil$. Since also $g(4\alpha) = 4\theta > \frac{3\pi}{2}$, $g(3\alpha) = 3\theta \geq \frac{9\pi}{8}$ and we therefore obtain that the length of $g(W_1)$ is at least

$$\frac{9\pi}{8} \frac{\left\lfloor \frac{3n}{8} \right\rfloor - \left\lceil \frac{n}{8} \right\rceil}{\left\lceil \frac{n}{8} \right\rceil} \geq \frac{9\pi}{4} \frac{n-6}{n+7} \geq 2\pi.$$

Consequently, $\bar{g}(W_1 \cap X) \cap V \neq \emptyset$ again a contradiction.

This finishes the proof for $v \neq 1$.

Case 2: $v = 1$ and $m \geq 3$. Let $\lambda = \frac{i}{m} = \frac{j}{m} - 1$, a positive integer. The slope of f is $\frac{j}{i} = 1 + \frac{1}{\lambda}$. Figure 3 shows the image $f\left[0, \frac{n}{j}\right]$ for $\lambda = 1, 2$ and 3. The greater λ the closer this image is to the diagonal D.

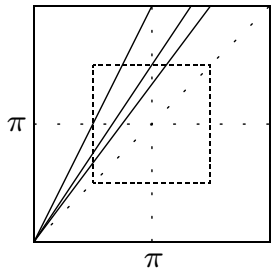

Figure 3

Suppose $m \geq 4$. Let t_0 be the greatest element of $\left[0, \frac{n}{4}\right] \cap X$ and t_1 the next element of X. Note that $t_1 - t_0 = \frac{n}{m} \leq \frac{n}{4}$ and hence $\frac{t_0+t_1}{2} = t_0 + \frac{t_1-t_0}{2} \leq \frac{3n}{8}$. Clearly $t_0 = \left\lfloor \frac{m}{4} \right\rfloor \frac{n}{m}$. So if $m \geq 6$ then $t_0 \geq \frac{m-3}{4}\frac{n}{m} \geq \frac{n}{8}$. On the other hand, if $m = 4$ or 5, then $t_0 = \frac{n}{m} \geq \frac{n}{5}$. So it follows that for $m \geq 4$, $I = \left[t_0, \frac{t_0+t_1}{2}\right] \subseteq W$. Because of condition (C3) we thus get $f(I \cap \mathbb{Z}) \cap V = \emptyset$. Set $k = \lfloor t_0 \rfloor + 1 \in W$. Then $0 < f_j(k) \leq \pi$ and thus $f_i(k) < \frac{\pi}{2}$ (Figure 3 is helpful here). Let p be the least non negative integer so that $f_i(k+p) \geq \frac{\pi}{2}$. Since $\pi \in f_i(I)$ (as at least half of circle is covered by $f_i(I)$), we have that $k + p \in I \cap \mathbb{Z}$ and so $f_j(k+p) > \frac{3\pi}{2}$.

Assume that $\lambda \neq 1$, of the possible lines representing $f\left[0, \frac{n}{j}\right]$ in Figure 3, the most left one is excluded. Then a look at the picture shows that $f_j(k+p) > \frac{3\pi}{2}$ implies that $f_i(k+p) > \pi$. So $s_i > \frac{\pi}{2}$. It then follows easily that $p = 1$. So $f_j(k+1) > \frac{3\pi}{2}$. Since $s_j \leq \pi$ we get that $f_j(k) > \frac{\pi}{2}$. A similar backward argument shows that $\pi \leq f_j(\lceil t_0 \rceil - 1) < \frac{3\pi}{2}$. Consequently, $|f_j(\lfloor t_0 \rfloor + 1) - f_j(\lceil t_0 \rceil - 1)| > \pi$. Using again that $s_j \leq \pi$ we thus get that the length of the interval $[\lceil t_0 \rceil - 1, \lfloor t_0 \rfloor + 1]$ is greater than 1 and hence t_0 is an integer. Therefore $\frac{\pi}{2} < f_i(k+1) - f_i(k) = f_i(t_0+1) - f_i(t_0) = f_i(k) < \frac{\pi}{2}$, a contradiction.

Thus $\lambda = 1$ and hence $j = 2i$ and $m = i$. Figure 4 represents the image of f and the curves C_1 and C_2 defined by the equations $\sin(x/2)\sin^2(y/2) = \frac{\sqrt{2}}{4}$ and $\sin^2(x/2)\sin(y/2) = \frac{\sqrt{2}}{4}$ respectively.

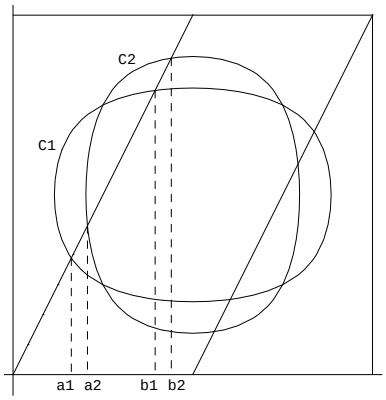

Figure 4

If (x, y) is in the region R_1 limited by the curve C_1 then $\sin(x/2)\sin^2(y/2) \geq \frac{\sqrt{2}}{4}$ and if (x, y) is in the region R_2 limited by C_2 then $\sin^2(x/2)\sin(y/2) \geq \frac{\sqrt{2}}{4}$. Let a_i and b_i be the first coordinates of the intersecting points of the first part of the image of f with C_i $(i = 1, 2)$. Because of condition (C2), there do not exist integers k_1 and k_2 in the interval W so that $f(k_i) \in R_i$ for both $i = 1, 2$. Hence it follows easily that $s_i > \min(b_1 - a_1, b_2 - a_2)$. Computing these intersections one obtains that

$$a_1 \leq 1.019, \quad a_2 \leq 1.302, \quad b_1 \geq 2.484, \quad b_2 \geq 2.766.$$

So $s_i > 1.464$ and thus $\frac{i}{n} = \frac{S}{2\pi} \geq 0.233$. As $n > 200$ we thus get $i > 46$ and hence $\alpha = \frac{n}{m} = \frac{n}{i} < \frac{n}{46}$. It follows that $\frac{n}{4} - \frac{n}{46} < t_0 < t_1 < \frac{n}{4} + \frac{n}{46}$. Consequently, for every $t \in [t_0, t_1]$ one has $\sin\frac{2\pi t}{n} \geq \sin\frac{21\pi}{46} > 0.9$. Let C_1' be the curve defined by the equation $\sin(x/2)\sin^2(y/2) = \frac{1}{4\cdot(0.9)}$ and C_2' the curve defined by $\sin^2(x/2)\sin(y/2) = \frac{1}{4\cdot(0.9)}$. Let a_i' and b_i' be the first components of the intersecting points of C_i' with the first part of the image of f. Then

$$a_1' \leq 0.912, \quad a_2' \leq 1.165, \quad b_1' \geq 2.573, \quad b_2' \geq 2.854.$$

Because of condition (C1), one obtains similarly as above that $s_j > 2\min(b_1' - a_1', b_2' - a_2') \geq 3.316 > \pi$, a contradiction.

So we have shown that $m = 3$. Let $t_0 = \left\lceil \frac{n}{3} \right\rceil$ and $k = t_0 - 1$. Similarly as in the previous situation (that is, for $m \geq 4$), one can now come to a contradiction arguing backward in the interval $\left[\frac{n}{6}, \frac{n}{3}\right]$.

Case 3: $mv \leq 2$. Let $I = [t_0, 2t_0] \cap W$ where $t_0 = \frac{\alpha}{4}$, so that

$$f(t_0) = \begin{cases} \left(0, \frac{\pi}{2}\right), \left(\frac{\pi}{2}, \pi\right), \left(\pi, \frac{3\pi}{2}\right) \text{ or } \left(\frac{3\pi}{2}, 0\right) & \text{if } v = 1 \\ \left(\frac{\pi}{4}, \frac{3\pi}{4}\right), \left(\frac{3\pi}{4}, \frac{5\pi}{4}\right), \left(\frac{5\pi}{4}, \frac{7\pi}{4}\right) \text{ or } \left(7\frac{\pi}{4}, \frac{\pi}{4}\right) & \text{if } v = 2 \end{cases}$$

For every $t \in I$, we have

$$\frac{\pi}{2} \leq f_j(t) - f_i(t) = \frac{2\pi t}{\alpha} \leq \pi.$$

Hence $f(I)$ is in the shadowed part of Figure 5 where the possible values for $f(t_0)$ have been represented by bold circles.

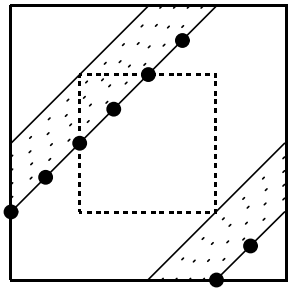

Figure 5

Moreover the slope s_{j-i} of the function $f_j - f_i$ is $\frac{2\pi(j-i)}{n} = \frac{2vm\pi}{n} < \frac{\pi}{50}$ (because by assumption $n > 200$).

The possible values of m and $f(t_0)$ leads to 12 different cases. Using similar arguments one can now show that each of these cases leads to a contradiction, and hence finishes the proof. Crucial in all these arguments is to understand what happens "shortly" after the time t_0. We illustrate the method for $m = 2$ and $f(t_0) = (0, \frac{\pi}{2}) = O$, so that $v = 1$.

Let $k = \lceil t_0 \rceil$. As $s_i \leq \pi$ and $s_{j-i} \leq \frac{\pi}{50}$ it thus follows that $0 \leq f_i(k) \leq \frac{7\pi}{8}$ and $\frac{\pi}{2} = f_j(t_0) - f_i(t_0) \leq f_j(k) - f_i(k) = (f_j - f_i(t_0)) + (f_j - f_i)(k - t_0) \leq \frac{\pi}{2} + \frac{\pi}{50} = \frac{13\pi}{25}$. Thus $\frac{\pi}{2} \leq f_j(k) \leq \frac{7\pi}{8} + \frac{13\pi}{25} < \frac{3\pi}{2}$. So, because of condition (C3) we obtain that $f_i(k) < \frac{\pi}{2}$. Let l be the first integer greater than t_0 so that $f_i(l) \geq \frac{\pi}{2}$. We claim that $f_i(l) \geq \frac{3\pi}{4}$. This is easy if $l \geq \frac{3n}{16}$, because $m = 2$ divides i and then $f_i(l) \geq \frac{2\pi i}{n}\frac{3n}{16} \geq \frac{3\pi}{4}$, as desired. So suppose that $l < \frac{3n}{16}$ and $f_i(l) < \frac{3\pi}{4}$. Then $f_j(l) = (f_j - f_i)(l) + f_i(l) < \frac{4\pi}{n}\frac{3n}{16} + \frac{3\pi}{4} = \frac{3\pi}{2}$. However this yields a contradiction with condition (C3). This proves the claim $f_i(l) \geq \frac{3\pi}{4}$. Hence it follows that $s_i \geq \frac{\pi}{4}$, and thus we get $l \leq k + 2$. If the slope of the image of f is S, then

$$\begin{aligned} 1 &< S = \frac{(f_j(l) - f_j(t_0))}{(f_i(l) - f_i(t_0))} = 1 + \frac{(f_j(l) - f_j(t_0)) - (f_i(l) - f_i(t_0))}{(f_i(l) - f_i(t_0))} = 1 + \frac{s_{j-i}(l - t_0)}{f_i(l)} \\ &< 1 + \frac{\frac{\pi}{50}(2 + \frac{7}{8})}{\frac{3\pi}{4}} = \frac{323}{300} = S_{\max}. \end{aligned}$$

Let a and b be the first two elements of I so that $A = f(a) = (A_1, A_2)$ and $B = f(b) = (B_1, B_2)$ belong to the curve C_1 with equation $\sin(x/2)\sin^2(y/2) = \frac{\sqrt{2}}{4}$, and let c and d the first two elements of I so that $C = f(c) = (C_1, C_2)$ and $D = f(d) = (D_1, D_2)$ belong to the curve C_2 with equation $\sin^2(x/2)\sin(y/2) = \frac{\sqrt{2}}{4}$. Figure 6 represents the curves C_1 and C_2 and the lines L_1 and L_2 through O of slopes 1 and S_{max} respectively.

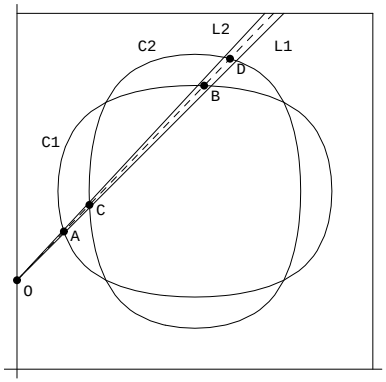

Figure 6

The image of an interval $[t_0, t_0+\epsilon]$ by f lies in the region between L_1 and L_2. Computing the intersections of the line through the point O and slopes 1 and $S_{\max}$ one deduces that

$$\begin{array}{rcl} 0.82 < & A_1 & < 0.84 \\ 1.27 < & C_1 & < 1.29 \\ 3.19 < & B_1 & < 3.44 \\ 3.65 < & D_1 & < 3.88 \end{array}$$

Condition (C2) implies that either $f_i(l-1) < A_1$ and $B_1 < f_i(l)$, or $f_i(l-1) < C_1$ and $D_1 < f_i(l)$. Thus $l-1-t_0 = \frac{(l-1)-t_0}{l-(l-1)} \leq \max\{\frac{A_1}{B_1-A_1}, \frac{C_1}{D_1-C_1}\} \leq 0.6$. In particular, $(l-1)-t_0 < 1$. Since also $l, k \in \mathbb{Z}$ and $t_0 \leq k \leq l-1$ we get that $l = k+1$ and $\lceil t_0 \rceil - t_0 = k - t_0 < 0.6$, so that $n \not\equiv 1,2,3 \mod 8$.

Arguing similarly in the interval $\left[\frac{5n}{8}, \frac{6n}{8}\right]$ (note that $f(\frac{5n}{8}) = 5f(t_0) = O$) one deduces that $5n \not\equiv 1,2,3 \mod 8$, so that $n \not\equiv 5,7 \mod 8$. If $n \equiv 0 \mod 8$ then $f(l) \in V$ contradicting (C3). We conclude that $n \equiv 4 \mod 8$ or $n \equiv 6 \mod 8$.

Condition (C2) implies that either $f_i(k) < A_1$ and $f_i(k+1) > B_1$, or $f_i(k) < C_1$ and $f_i(k+1) > D_1$. Therefore $s_i > \min(B_1 - A_1, D_1 - C_1) \geq 2.35$.

Assume that $n \equiv 4 \mod 8$. Then $f_i(k) = s_i/2 > 2.35/2 > A_1$ and hence $f_i(k) < C_1$ and $f_i(k+1) > D_1$. The first implies that $s_i < 2C_1 < 2.58$ and the second implies that $s_i > \frac{2D_1}{3} > 2.43$. Therefore, we have

$$2\pi + \frac{\pi}{2} < \frac{7 \cdot 2.43}{2} < f_i(k+3) = \frac{7s_i}{2} < \frac{7 \cdot 2.58}{2} < 2\pi + \frac{3\pi}{2}$$

and

$$2\pi+\frac{\pi}{2} < \frac{7 \cdot 2.43}{2}+\frac{\pi}{2} < f_i(k+3)+\frac{\pi}{2} < f_j(k+3) < f_i(k+3)+\frac{\pi}{2}+\frac{7\pi}{2}\frac{\pi}{50} < \frac{7 \cdot 2.58}{2}+\frac{\pi}{2}+\frac{7}{2}\frac{\pi}{50} < 2\pi+\frac{3\pi}{2}.$$

So $f(k+3) \in V$ which yields to a contradiction with (C3).

So $n \equiv 6 \mod 8$. Then $5s_i/4 = f_i(k+1) > B_1 > 3.19$, so that $s_i > 2.55$. Let $h = \lceil \frac{n}{4} \rceil = \frac{n+2}{4}$. Then $\frac{\pi}{2} < f_1(h) = \frac{\pi(n+2)}{2n} < \frac{\pi}{2}+\frac{\pi}{200} = \frac{102\pi}{200}$, $1.27 < s_i/2 = f_i(h) < \frac{\pi}{2}$ and $\pi < f_j(h) \leq f_i(h)+\pi+\frac{\pi}{100}$, so that

$$\min\{|\sin f_1(h) \sin f_i(h/2) \sin^2 f_{j/2}(h/2)|, |\sin f_1(h) \sin^2 f_i(h/2) \sin f_{j/2}(h/2)|\} \geq$$

$$\sin \tfrac{102\pi}{200} \sin^2 \tfrac{1.27}{2} \sin \tfrac{(1.27+101\pi/100)}{2} > \tfrac{1}{4},$$

which yields to a contradiction with (C1). ∎

4 Final Remarks

From the first part of the paper it is clear that the problem of the freeness of the group generated by two bicyclic units is usually a consequence of a problem of determining when the group generated by two 2×2-matrices is a free group. In particular, with notation as in Proposition 2.4, to ensure that the group $G = \langle 1+a, 1+b \rangle$ is free of rank 2 it is enough to show that the two matrices

$$\begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix} \quad \begin{pmatrix} 1 & 0 \\ \lambda & 1 \end{pmatrix}$$

generate a free group, where $2\lambda = \mathrm{tr}(\rho(ab)) \in \mathbb{C}$. If this is the case it is common to say that λ is a free point [1]. So far we have used Sanov's Theorem that states that a complex number of modulus at least 2 is a free point. The problem of deciding when a complex number is a free point is an active topic of research. For numerous complex numbers it has been determined whether they are free or not. For an up to date list we refer to [1].

Recently Bamberg [1] has given a family F of polynomials so that a point is free if and only if it is the root of an element of F. However, it is very difficult to check if a particular λ is root of one of the given polynomials. In particular we don't know if $\sqrt{3}$ is a free point. We now outline that an answer to the latter is needed to deal with bicyclic units of arbitrary dihedral groups.

Let b_1, b_2 be two non commuting bicyclic units of the same type in $\mathbb{Z}D_n$. It is again easily seen that we may assume that $b_1 = \beta_{a^t,b}$ and $b_2 = \beta_{a^i,a^jb}$. If $x = (b_1 - 1)(b_2 - 1)$, then (with the notation of Section 3)

$$\chi_k(x) = 16 \sin \frac{2\pi tk}{n} \sin \frac{2\pi ik}{n} \sin^2 \frac{\pi jk}{n}.$$

In general it is not true that there is k so that $\chi_k(x) \geq 4$. For example, if $n = 12$, $t = j = 2$ and $i = 3$, then $\chi_k(x) = 0$ if $k = 2, 3, 4$ and $|\chi_k(x)| = 2\sqrt{3} < 4$ if $k = 1, 5$. Let us look at the representations. The Wedderburn decomposition of $\mathbb{Q}D_{12}$ is well known:

$$\mathbb{Q}D_{12} = 4\mathbb{Q} \oplus 3M_2(\mathbb{Q}) \oplus M_2(\mathbb{Q}(\sqrt{3})).$$

Taking appropriate basis one may make the following identifications:

$$b_1 = (1, 1, 1, 1, A, A, 1, C) \quad \text{and} \quad b_2 = (1, 1, 1, 1, 1, B, D),$$

where $A, B \in M_2(\mathbb{Q})$ are non-identity matrices so that $(A-1)^2 = (B-1)^2 = 0$, and

$$C = \begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix} \quad \text{and} \quad D = \begin{pmatrix} 1 & 0 \\ \sqrt{3} & 1 \end{pmatrix}.$$

Thus $\langle b_1, b_2 \rangle$ is free if and only if there do not exist non zero integers $h_1, \ldots, h_m$ and $k_1, \ldots, k_m$ so that

$$h_1 + \ldots + h_m = k_1 + \ldots + k_m = 0 \quad \text{and} \quad C^{h_1} D^{k_1} C^{h_2} D^{k_2} \ldots C^{h_m} D^{k_m} = I.$$

In particular if $\sqrt{3}$ is a free point then $\langle b_1, b_2 \rangle$ is free.

Actually the previous case seems to be the only problematic case in dihedral groups. Indeed, a computer search for $n \leq 200$ shows that if n is not a multiple of 12 then for every $1 \leq t, i, j < n$ there exists a k so that $|\chi_k(x)| \geq 4$. Moreover if $n = 12m$ then the only values of (t, i, j) for which $|\chi_k(x)| < 4$ for every value of k are

$$(2, 3, 2)m, \quad (3, 2, 2)m, \quad (4, 3, 2)m \quad \text{and} \quad (3, 4, 2)m.$$

After an appropriate reduction one can show that all the cases reduce to $n = 12$ and $(t, i, j) = (2, 3, 2)$. This is precisely the example dealt with above. So, this seems to be an indication that for every two non commuting bicyclic units b_1 and b_2 of the same type in $\mathbb{Z}D_n$ one has that $\langle b_1, b_2^2 \rangle$ is a free group and if $\sqrt{3}$ is a free point then $\langle b_1, b_2 \rangle$ is always free.

We finish with a remark on the group generated by two bicyclic units of different type. Let $b_1 = \beta_{a,b}$ and $b_2 = \gamma_{a^i,a^jb}$. Then for every irreducible complex character χ_k of D_n we get

$$\chi_k(x) = 16 \sin \frac{2\pi k}{n} \sin \frac{2\pi ik}{n} \cos^2 \frac{\pi jk}{n}.$$

However, for this formula there is no analogue of Lemma 3.1. Indeed, for $n = 3$, that is for D_3, there are pairs of bicyclics with "bad" trace. For example, if $b_1 = \beta_{a,b}$ and $b_2 = \gamma_{a,ab}$, then

$$\chi_1(x) = 16 \sin \frac{2\pi}{3} \sin \frac{2\pi}{3} \cos^2 \frac{\pi}{3} = 3.$$

This implies that $\langle b_1, b_2 \rangle$ is not free. Actually as mentioned in [2] the group $\langle b_1, b_2 \rangle$ contains the trivial unit $a \in D_3$.

Acknowledgment. We would like to express our gratitude to Victor Jimnez for some helpful conversation on inequality (3.1).

References

[1] J. Bamberg, *Non-free points for groups generated by a pair of 2×2 matrices*, J. London Math. Soc. (2) 62 (2000) 795–801.

[2] A. Dooms and E. Jespers, Normal complements of the trivial units in the unit group of some some integral group rings, preprint.

[3] E. Jespers and G. Leal, Generators of large subgroups of the unit group of integral group rings, Manuscripta Math. 78 (1993), 303–315.

[4] Z.S. Marciniak and S.K. Sehgal, *Constructing free subgroups of integral group rings* Proc. AMS 125 (1997), 1005–1009.

[5] J. Ritter and S.K. Sehgal. *Generators of Subgroups of* $U(\mathbb{Z}G)$, Contemporary Math. 93 (198) 331–347.

[6] J. Ritter, S.K. Sehgal, Construction of units in integral group rings of finite nilpotent groups, Trans. Amer. Math. Soc. 324 (2) (1991), 603–621.

[7] A. Salwa, *On free subgroups of units of rings*, preprint.

[8] I.N. Sanov, *A property of a representation of a free group*, Doklady Akad. SSSR 57 (1947) 657–659.