Abstract

In 1926, Jarník introduced the problem of drawing a convex \( n \)-gon with vertices having integer coordinates. He constructed such a drawing in the grid \([1, c \cdot n^{3/2}]^2\) for some constant \( c > 0 \), and showed that this grid size is optimal up to a constant factor. We consider the analogous problem for drawing the double circle, and prove that it can be done within the same grid size. Moreover, we give an \( O(n) \)-time algorithm to construct such a point set.

1 Introduction

Given \( n \geq 3 \), a double circle is a set \( P = \{p_0, p_1, \ldots, p_{n-1}, p'_0, p'_1, \ldots, p'_{n-1}\} \) of \( 2n \) planar points in general position such that: (1) \( p_0, p_1, \ldots, p_{n-1} \) are precisely the vertices of the convex hull of \( P \) labelled in counterclockwise order around the boundary; (2) point \( p'_i \) is close to the segment joining \( p_i \) with \( p_{i+1} \); (3) the line passing through \( p_i \) and \( p'_i \) separates \( p_{i+1} \) from \( P \); and (4) the line passing through \( p'_i \) and \( p_{i+1} \) separates \( p_i \) from \( P \) (see Figure 1). Subindices are taken modulo \( n \). The double circle has been considered in combinatorial geometry and it is conjectured to have the least number of triangulations [1, 2].
Drawing an $n$-vertex convex polygon with integer vertices can be easily done by considering the $n$ points $(1, 1), (2, 4), (3, 9), \ldots, (n, n^2)$ as the vertices of the polygon. In this case the size of the integer point set is equal to $n^2 - 1 = \Theta(n^2)$, where size refers to the smallest $N$ such that the point set can be translated to lie in the grid $[0, N]^2$. In 1926, Jarník [5] showed how to draw an $n$-vertex convex polygon with size $N = O(n^{3/2})$ and proved that this bound is optimal. In recent years the so-called Jarník polygons and extensions of them have been studied [3, 6].

Given any integer point $(i, j)$, we say that $(i, j)$ is visible (from the origin) if the interior of the line segment joining the origin and $(i, j)$ contains no lattice points. Observe that $(i, j)$ is visible if and only if $\gcd(i, j) = 1$, where $\gcd(i, j)$ denotes the greatest common divisor of $i$ and $j$. We consider points as vectors as well, and vice versa. A Jarník polygon is formed by choosing a natural number $Q$, and taking the set $V_Q$ of visible vectors $(i, j)$ such that $\max\{|i|, |j|\} \leq Q$ [4, 5, 6]. The polygon is then the unique (up to translation) convex polygon whose edges, viewed as vectors, are precisely the elements of $V_Q$, that is, the vertices can be obtained by starting from an arbitrary point and adding the vectors of $V_Q$, one by one, in counterclockwise order, to the previously computed vertex (see Figure 2).
the smallest size $N$. We present an $O(n)$-time algorithm that correctly constructs the double circle with size within $O(n^{3/2})$, where that bound is also optimal. We consider the unit cost RAM model, where all operations with real numbers, including the floor and ceiling functions, require constant time. In Section 2 we show our algorithm, and in Section 3 its correctness is proved. Finally, in Section 4 we state future work. Some examples are given in Appendix A.

2 Double circle construction

Observe that a simple construction with quadratic size is as follows: Consider the function $f(x) = x^2 + x$. For $i = 1, \ldots, 2n - 1$, add the point $(i, f(i))$ if $i$ is odd, and the point $(i, f(i) + 2)$ otherwise. The final point is $(n, \frac{f(2n-1)+f(1)}{2}) = (n, 2n^2 - n)$, i.e., the point just below the midpoint of the segment connecting $(1, f(1))$ and $(2n-1, f(2n-1))$. The size of the resulting point set is $N = f(2n-1) - f(1) = (2n-1)^2 + (2n-1) - 2 = 4n^2 - 2n - 2 = \Theta(n^2)$.

We say that a sequence $V$ of vectors is symmetric if $V$ contains an even number of vectors sorted counterclockwise around the origin, and for every vector $a$ in $V$ its opposite vector $-a$ is also in $V$. Observe that any sequence of vectors defining a Jarník polygon is symmetric. For any sequence $V = [v_1, v_2, \ldots, v_{2t}]$ of $2t$ vectors let the point set $P(V) := \{p_1, p_2, \ldots, p_{2t}\}$, where $p_1 = v_1$ and $p_i = p_{i-1} + v_i$ for $i = 2, \ldots, 2t$. Note that if we sort the elements of $V_Q$ around the origin then the elements of $P(V_Q)$ are the vertices of the Jarník polygon. Furthermore, if $V$ is symmetric then the elements of $P(V)$ are in convex position. Let sequence $\text{alt}(V) := [v_2, v_1, v_4, v_3, \ldots, v_{2t}, v_{2t-1}]$ (see Figure 3 for an example with $t = 8$). For any scalar $\lambda$ let the sequence $\lambda V := [\lambda v_1, \lambda v_2, \ldots, \lambda v_{2t}]$.

![Figure 3: $P(\text{alt}(V))$](image)

The idea is to generate a suitable symmetric sequence $V$ of $2n$ vectors...
and then build the point set $P(\text{alt}(V))$ as the double circle point set, up to some transformation of the elements of $\text{alt}(V)$. A (not optimal) example is $V = [(1,1), (1,2), \ldots, (1,n), (-1,-1), (-2,-2), \ldots, (-1,n)]$ for even $n \geq 4$. The point set $P(\text{alt}(V))$ is in fact a double circle but its size is equal to $1 + 2 + \ldots + n = \Theta(n^2)$ (see Figure 4).

![Figure 4](image)

Figure 4: A naive construction for $n = 4$ showing both vectors (left) and the resulting point set (right).

The construction in which the resulting point set is a double circle of size $O(n^{3/2})$ is based on the next two algorithms:

**VisibleVectors($n$):** With input $n \geq 3$, the symmetric sequence $V$ of $2n$ visible vectors, sorted counterclockwise around the origin, is generated so as to satisfy the next two invariants. Let $B_t := \{p \in \mathbb{Z}^2 : \|p\|_1 \leq t\}$, $k := \max_{v \in V} \|v\|_1$, and (even) $s$ be the number of visible vectors of $B_{k-1}$: (i) all visible vectors of $B_{k-1}$ are in $V$, and (ii) the other elements of $V$ are generated as follows, until $2n - s$ elements are obtained: for $i = 1, \ldots, k - 1$ generate vectors $(i,k-i)$, $(-i,-(k-i))$, $(-i,k-i)$, $(i,-(k-i))$ in this order, if and only if gcd$(i,k-i) = 1$. Refer to Algorithm 2.1 for a pseudo-code.

**BuildDoubleCircle($n$):** With input $n \geq 3$, build a $2n$-point double circle. First, set sequences $V := \text{VisibleVectors}(n)$ and $[v'_1, v'_2, \ldots, v'_{2n}] := \text{alt}(V)$. Then, the sequence $W = [w_1, w_2, \ldots, w_{2n}]$ of $2n$ vectors is created as follows: for $i = 1, 3, \ldots, 2n - 1$ set $w_i = (1 - \lambda)v'_i + \lambda v'_{i+1}$ and $w_{i+1} = \lambda v'_i + (1 - \lambda)v'_{i+1}$, where $\lambda = 1/3$. Finally, build the $2n$-point set $P((1/\lambda)W)$ as the double circle.
Algorithm 2.1: \textsc{VisibleVectors}(n)

\begin{verbatim}
\begin{algorithmic}
\State \textbf{repeat}
\State \hspace{1em} $k \leftarrow 1$
\State \hspace{1em} $V \leftarrow \{(1,0), (-1,0), (0,1), (0,-1)\}$
\State \hspace{1em} \textbf{repeat}
\State \hspace{2em} \hspace{1em} $k \leftarrow k + 1$
\State \hspace{2em} \hspace{1em} \textbf{for} $i \leftarrow 1$ \textbf{to} $k - 1$
\State \hspace{2em} \hspace{2em} \hspace{1em} \textbf{if} $\text{gcd}(i,j) = 1$
\State \hspace{2em} \hspace{2em} \hspace{2em} \hspace{1em} \textbf{do}
\State \hspace{2em} \hspace{2em} \hspace{2em} \hspace{2em} \hspace{1em} \hspace{1em} \textbf{if} $\text{length}(V) < 2n$
\State \hspace{2em} \hspace{2em} \hspace{2em} \hspace{2em} \hspace{2em} \hspace{2em} \hspace{1em} \hspace{1em} \textbf{then} $V \leftarrow V + [(i,j), (-i,-j)]$
\State \hspace{2em} \hspace{2em} \hspace{2em} \hspace{2em} \hspace{2em} \hspace{2em} \hspace{1em} \hspace{1em} \textbf{if} $\text{length}(V) < 2n$
\State \hspace{2em} \hspace{2em} \hspace{2em} \hspace{2em} \hspace{2em} \hspace{2em} \hspace{2em} \hspace{1em} \hspace{1em} \textbf{then} $V \leftarrow V + [(-i,j), (i,-j)]$
\State \hspace{2em} \hspace{2em} \hspace{2em} \hspace{2em} \hspace{1em} \textbf{until} \ $\text{length}(V) = 2n$
\State \hspace{1em} \textbf{Sort} $V$ \textbf{counterclockwise around origin}
\State \hspace{1em} \textbf{return} $(V)$
\end{algorithmic}
\end{verbatim}

3 Construction correctness

Let $V = [v_1, v_2, \ldots, v_{2n}]$ be the (circular) sequence of vectors obtained by executing \textsc{VisibleVectors}(n), for $n \geq 3$. For every $i = 1, 3, 5, \ldots, 2n - 1$ we say that the pair of vectors $v_i, v_{i+1}$ is a pair of $\text{alt}(V)$.

\textbf{Lemma 1} (Chapter 2 of [4]). Given a natural number $Q$, the number $|V_Q|$ of vertices of the Jarník polygon is equal to

$$4 + 4 \sum_{i=1}^{Q} \sum_{j=1}^{Q} \frac{1}{\text{gcd}(i,j)} = \frac{24Q^2}{\pi^2} + O(Q \log Q).$$

The size $S(Q)$ of the Jarník polygon is equal to

$$1 + 2 \sum_{i=1}^{Q} \sum_{j=1}^{Q} \frac{i}{\text{gcd}(i,j)} = 1 + 2 \sum_{i=1}^{Q} \sum_{j=1}^{Q} \frac{j}{\text{gcd}(i,j)} = \frac{6Q^3}{\pi^2} + O(Q^2 \log Q).$$

\textbf{Lemma 2}. $V$ is symmetric and point set $\mathcal{P}(V)$ has size $O(n^{3/2})$.

\textit{Proof}. Observe that for every vector $a$ in $V$, $-a$ is also in $V$ since in algorithm \textsc{VisibleVectors} the vectors are added to sequence $V$ in pairs, and each pair consists of two opposite vectors. Then $V$ becomes symmetric once the elements of $V$ are sorted counterclockwise around the origin. On the other hand $V_{\lfloor \frac{k}{2} \rfloor} \subset V \subset V_k$, where $k = \max_{v \in V} \|v\|_1$. Then we have
\[ |V_{k+1}| \leq 2n \leq |V_k|, \text{ which implies } k = \Theta(\sqrt{n}) \text{ by Lemma 1.} \]

By the same lemma we obtain:

\[
\sum_{i=1}^{n} x(v_i), \sum_{i=1}^{n} y(v_i) < 1 + 2 \sum_{i=1}^{k} \sum_{j=1}^{k} i \quad \text{gcd}(i,j) = 1
\]

\[
= S(k)
\]

\[
\Theta(k^3) = \Theta(n^{3/2})
\]

Hence, the size of \( \mathcal{P}(V) \) is \( O(n^{3/2}) \).

Let \( o \) denote the origin of coordinates. Given two points \( p, q \) let \( \ell(p,q) \) denote the line passing through \( p \) and \( q \) and directed from \( p \) to \( q \), and \( pq \) denote the segment joining \( p \) and \( q \). Given three points \( p = (x_p, y_p), q = (x_q, y_q), \) and \( r = (x_r, y_r) \), let \( \Delta(p,q,r) \) denote the triangle with vertices at \( p, q, \) and \( r; \) \( A(p,q,r) \) denote the area of \( \Delta(p,q,r) \); and \( \text{turn}(p,q,r) \) denote the so-called geometric turn (going from \( p \) to \( r \) passing through \( q \)) where

\[
\text{turn}(p,q,r) = \begin{vmatrix} x_p & y_p & 1 \\ x_q & y_q & 1 \\ x_r & y_r & 1 \end{vmatrix}
\]

and \( A(p,q,r) = \frac{1}{2} |\text{turn}(p,q,r)| \). Extending this notation, let \( \Delta(p,q) := \Delta(o,p,q) \), \( A(p,q) := A(o,p,q) \), and \( \text{turn}(p,q) := \text{turn}(o,p,q) \). We use the so-called Pick’s theorem:

**Theorem 3** (Pick’s theorem). The area of any simple polygon \( H \) with lattice vertices is equal to \( i + b/2 - 1 \), where \( i \) and \( b \) are the numbers of lattice points in the interior and the boundary of \( H \), respectively.

**Lemma 4.** For every two consecutive vectors \( a_1, a_2 \) of \( V \) we have \( A(a_1,a_2) = 1/2 \).

**Proof.** Suppose \( \Delta(a_1,a_2) \) contains a lattice point \( p \) different from \( o, a_1, \) and \( a_2 \). Then \( p \) cannot belong to segments \( oo_1 \) and \( oo_2 \), and segment \( op \) contains a visible point \( q \) (possibly equal to \( p \)). If \( \|q\|_1 < \max\{\|a_1\|_1, \|a_2\|_1\} \) then \( q \) must belong to \( V \) by invariant (i) of algorithm \( \text{VISIBLEVECTORS} \). Otherwise, we have \( \|q\|_1 = \max\{\|a_1\|_1, \|a_2\|_1\} \). Suppose w.l.o.g. that \( \|a_1\|_1 < \|a_2\|_1 \), and let the point \( q' \) denote the intersection of \( \ell(o,q) \) with the segment \( s \) connecting \( a_1 \) to \( a_2 \). Observe that \( q' = \delta a_1 + (1-\delta)a_2 \) for some \( \delta \in (0,1) \), and further that \( \|q\|_1 \leq \|q'\|_1 = \|\delta a_1 + (1-\delta)a_2\|_1 \leq \delta \|a_1\|_1 + (1-\delta)\|a_2\|_2 < \|a_2\|_1 \), which is a contradiction. Then we must have that \( \|q\|_1 = \|a_1\|_1 = \|a_2\|_1 \), which implies that \( q, a_1, a_2 \) belong to a same quadrant since in this case \( q \) is at the interior of the segment \( s \). Therefore, \( q \) must belong to \( V \) by invariant (ii) of algorithm \( \text{VISIBLEVECTORS} \). In both cases, the fact that \( q \) belongs to \( V \) contradicts the fact that \( a_1 \) and \( a_2 \) are consecutive vectors of \( V \). Hence \( A(a_1,a_2) = 1/2 \) by Pick’s theorem. \( \square \)
Let $\lambda \in (0, 1/2)$. Given a pair $a, b$ of vectors let $h(\lambda, a, b) := (1 - \lambda)a + \lambda b$ (see Figure 5).

Figure 5: Two vectors $a$ and $b$, and the vectors $h(\lambda, a, b)$ and $h(\lambda, b, a)$.

**Lemma 5.** Let $a_1, a_2, a_3, a_4$ be four consecutive vectors of $V$ such that $a_1, a_2$ and $a_3, a_4$ are pairs of alt($V$). Let $\lambda \in (0, 1/2)$, $q_1 = h(\lambda, a_2, a_1)$, $q_2 = q_1 + h(\lambda, a_1, a_2)$, $q_3 = q_2 + h(\lambda, a_4, a_3)$, and $q_4 = q_3 + h(\lambda, a_3, a_4)$. Then $q_2$ is to the right of $\ell(o, q_1)$ and both $q_3$ and $q_4$ are to the left of $\ell(o, q_1)$.

**Proof.** (Refer to Figure 6) We have that:

$$\text{turn}(q_1, q_2) = \text{turn}(q_1, q_1 + h(\lambda, a_1, a_2))$$
$$= \text{turn}((1 - \lambda)a_2 + \lambda a_1, a_1 + a_2)$$
$$= (1 - \lambda)\text{turn}(a_2, a_1) + \lambda \text{turn}(a_1, a_2)$$
$$= 2(2\lambda - 1)A(a_1, a_2)$$
$$< 0,$$

which implies that $q_2$ is to the right of the line $\ell(o, q_1)$. On the other hand:

Figure 6: Proof of Lemma 5.
\[
\text{turn}(q_1, q_3) = \text{turn}(h(\lambda, a_2, a_1), h(\lambda, a_2, a_1) + h(\lambda, a_1, a_2) + h(\lambda, a_4, a_3)) \\
= \text{turn}(h(\lambda, a_2, a_1), h(\lambda, a_1, a_2)) + \\
\text{turn}(h(\lambda, a_2, a_1), h(\lambda, a_4, a_3)) \\
= \text{turn}((1 - \lambda)a_2 + \lambda a_1, (1 - \lambda)a_1 + \lambda a_2) + \\
\text{turn}((1 - \lambda)a_2 + \lambda a_1, (1 - \lambda)a_4 + \lambda a_3) \\
= (1 - \lambda)^2 \text{turn}(a_2, a_1) + \lambda^2 \text{turn}(a_1, a_2) + \\
(1 - \lambda)^2 \text{turn}(a_2, a_4) + \lambda(1 - \lambda) \text{turn}(a_2, a_3) + \\
\lambda(1 - \lambda) \text{turn}(a_1, a_4) + \lambda^2 \text{turn}(a_1, a_3) \\
= 2\left((2\lambda - 1)A(a_1, a_2) + (1 - \lambda)^2 A(a_2, a_4) + \\
\lambda(1 - \lambda)A(a_2, a_3) + \lambda(1 - \lambda)A(a_1, a_4) + \\
\lambda^2 A(a_1, a_3)\right) \\
= 2\left(\frac{1}{2} (2\lambda - 1) + (1 - \lambda)^2 A(a_2, a_4) + \\
\lambda(1 - \lambda)A(a_2, a_3) + \lambda(1 - \lambda)A(a_1, a_4) + \\
\lambda^2 A(a_1, a_3)\right) \\
\geq (2\lambda - 1) + (1 - \lambda)^2 + \lambda(1 - \lambda) + \\
\lambda(1 - \lambda) + \lambda^2 \\
= 2\lambda > 0
\]

where equation [1] follows from Lemma [4] and equation [2] follows from the fact that by Pick’s theorem the area of any non-empty triangle with lattice vertices is at least 1/2. Therefore \(q_3\) is to the left of \(\ell(o, q_1)\). Similarly, since we have that \(\text{turn}(a_i, a_j) > 0\) \((i = 1, 2; j = 3, 4)\) then

\[
\text{turn}(h(\lambda, a_2, a_1), h(\lambda, a_3, a_4)) > 0,
\]

which implies that \(q_4\) is to the left of \(\ell(o, q_1)\) given that \(q_3\) is to the left of \(\ell(o, q_1)\). By symmetry, it can be proved that \(\text{turn}(q_4, q_3, q_1) < 0\) and \(\text{turn}(q_4, q_3, o) < 0\), implying that both \(q_1\) and \(o\) are to the right of \(\ell(q_4, q_3)\).

Lemma 6. Algorithm \texttt{VisiblePoints} can be implemented to run in \(O(n)\) time in the unit cost RAM model, \(n \geq 3\).

\textbf{Proof.} Let \(n \geq 3\) and \(V\) be the answer of calling \texttt{VisiblePoints}(\(n\)). Let \(m := 1 + \max_{e \in V} |e|_1\) which satisfies \(m = \Theta(\sqrt{n})\) (see the proof of Lemma [2]). Using \(O(m^2)\) space, and the facts \(\gcd(i, i) = i\) and \(\gcd(i, j) = \gcd(i - j, j)\) for \(i > j\), one can compute \(\gcd(i, j)\) in constant time for any \(i, j\). Then, computing \(V\) without the radial sorting around the origin requires \(O(m^2) = O(n)\) time.
We show now that $V$ can be radially sorted around the origin in $O(n)$ time via Bucket Sort, and it suffices to show how to sort the vectors $V′ \subset V$ that belong to the interior of the first quadrant. Let $b_t$ denote the point $(t/m, m - t/m)$ for $t = 0, 1, \ldots, m^2$, and consider the $m^2$ triangles $\Delta_1, \Delta_2, \ldots, \Delta_{m^2}$ as buckets, where triangle $\Delta_t$ ($t = 1, \ldots, m^2$) has vertices $o, b_{t-1},$ and $b_t$. Observe that triangles $\Delta_1, \Delta_2, \ldots, \Delta_{m^2}$ have pairwise disjoint interiors, and all have area equal to $1/2$. If $a_1$ and $a_2$ are two different vectors of $V′$ then $A(o, a_1, a_2) \geq 1/2$, which implies that $a_1$ and $a_2$ cannot belong to a same triangle (bucket) $\Delta_t$ given that both are not contained in the segment $b_{t-1}b_t$ for $t = 1, \ldots, m^2$. Therefore, every triangle among $\Delta_1, \Delta_2, \ldots, \Delta_{m^2}$ contains at most one point of $V′$. Given any vector $a := (i, j) \in V′$, the triangle $\Delta_t$ that contains $(i, j)$ can be found in constant time. Namely, $t$ is the smallest value in the range $[1 \ldots m^2]$ such that
\[
\begin{vmatrix}
0 & 0 & 1 \\
1 & j & 1 \\
t/m & m - t/m & 1
\end{vmatrix} = i(m - t/m) - j(t/m) \leq 0
\]
\[
i \cdot \frac{m^2}{i + j} \leq t
\]
where $t$ satisfies $t = \lceil \frac{im^2}{i + j} \rceil$. Since $t$, and then $\Delta_t$, can be found in constant time, the vectors of $V′$ can be sorted in $O(m^2) = O(n)$ time.

\[\textbf{Theorem 7.} \text{ There is an } O(n) \text{-time algorithm that for all } n \geq 3 \text{ builds a double circle of } 2n \text{ points in the grid } [0, N]^2 \text{ where } N = O(n^{3/2}).\]

\[\textbf{Proof.} \text{ Execute the algorithm } \text{BUILDDOUBLECIRCLE} \text{ with input } n, \text{ being } V \text{ the result of calling } \text{VISIBLEPOINTS}(n), \text{ building the point set } P \text{ of } 2n \text{ points. Observe that } \lambda = 1/3 \text{ implies that point } w_i/\lambda = 3w_i \text{ is integer for } i = 1 \ldots 2n, \text{ and then all elements of } P \text{ are integer points. By Lemma 5, the point set } P \text{ is a double circle. The size of } P(V) \text{ is } O(n^{3/2}) \text{ by Lemma 2 and since all elements of } P \text{ belong to the polygon with vertices } P(3V), \text{ the size } N \text{ of } P \text{ is also } O(n^{3/2}). \text{ Finally, translate } P \text{ to lie in the grid } [0, N]^2. \text{ Since algorithm } \text{VISIBLEPOINTS} \text{ can run in } O(n) \text{ time (Lemma 6), algorithm } \text{BUILDDOUBLECIRCLE} \text{ can be done in } O(n) \text{ time. The result follows.}\]

\[\textbf{4 Future work}\]

We are working on extending the results of this paper to build other known point sets in integer points of small size, such as the double convex chain, the Horton set, and others. We plan to eventually release a software library supporting many of these constructions.
References

[1] O. Aichholzer, F. Hurtado, and M. Noy. A lower bound on the number of triangulations of planar point sets. *Computational Geometry*, 29(2):135–145, 2004.

[2] O. Aichholzer, D. Orden, F. Santos, and B. Speckmann. On the number of pseudo-triangulations of certain point sets. *Journal of Combinatorial Theory, Series A*, 115(2):254–278, 2008.

[3] I. Bárány and N. Enriquez. Jarník's convex lattice $n$-gon for non-symmetric norms. *Mathematische Zeitschrift*, 270:627–643, 2012.

[4] M. N. Huxley. *Area, lattice points, and exponential sums*. Oxford Science Publications. The Clarendon Press Oxford University Press, New York, 1996.

[5] V. Jarník. Über die Gitterpunkte auf konvexen Kurven. *Mathematische Zeitschrift*, 24:500–518, 1926.

[6] G. Martin. The Limiting Curve of Jarník's Polygons. *Transactions of the American Mathematical Society*, 355(12):4865–4880, 2003.

[7] G. Pick. Geometrisches zur Zahlenlehre. *Sitzungsberichte des Deutschen Naturwissenschaftlich-Medicinischen Vereines für Böhmen “Lotos” in Prag.*, 19:311–319, 1899.
A Examples

Figure 7: Output of the algorithm for $n = 3, 4, 5, 6$ (right) and the corresponding vectors $W$ (left).
Figure 8: Vectors of sequence $W$ for $n = 256, 512, 1024$. 

12