ACTA ET COMMENTATIONES UNIVERSITATIS TARTUENSIS DE MATHEMATICA
Volume 24, Number 1, June 2020
Available online at http://acutm.math.ut.ee

Complexities of self-dual normal bases

Stéphane Blondeau Da Silva

Abstract. The complexities of self-dual normal bases, which are candidates for the lowest complexity basis of some defined extensions, are determined with the help of the number of all but the simple points in well chosen minimal Besicovitch arrangements. In this article, these values are first compared with the expected value of the number of all but the simple points in a minimal randomly selected Besicovitch arrangement in ${\mathbb{F}_d}^2$ for the first 370 prime numbers d. Then, particular minimal Besicovitch arrangements which share several geometrical properties with the arrangements considered to determine the complexity are considered in two distinct cases.

1. Introduction

Let q be a prime power, $\mathbb{F}_q$ be the field of q elements and n be a positive integer. We consider the Galois group of the extension $\mathbb{F}_{q^n}/\mathbb{F}_q$, which is a cyclic group generated by the Frobenius automorphism $\Phi : x \mapsto x^q$. There exists an α that generates a "normal" basis for $\mathbb{F}_{q^n}/\mathbb{F}_q$, i.e., a basis consisting of the orbit $(\alpha, \alpha^q, \dots, \alpha^{q^{n-1}})$ of α under the action of the Frobenius (see the recent book of Mullen and Panario [17]). Normal bases are widely used in applications of finite fields in domains such as signal processing, coding theory, cryptography, etc. (see [14]). The difficulty of multiplying two elements of the extension expressed in such bases is measured by the complexity of α, namely the number of non-zero entries in the multiplication-by-α matrix [16, 4.1]. As a large number of zeros in this matrix enables faster calculations, finding normal bases with low complexity is a significant issue [2]. Mullin et al. [18] proved that the complexity is at least $2n-1$. When this value is reached, the basis is optimal. Optimal normal bases over finite fields were completely characterized by Gao and Lenstra [10] (see also [6, 9, 23]). But such bases do not exist for all finite fields and all extensions [12].

Received June 8, 2019.
2010 *Mathematics Subject Classification.* 51E99.
Key words and phrases. Self-dual normal basis, complexity, Besicovitch arrangement.
https://doi.org/10.12697/ACUTM.2020.24.05

Self-dual normal bases are particular normal bases which verify, for $0 \leq i, j \leq n-1$, $Tr(\alpha^{q^i}\alpha^{q^j}) = \delta_{i,j}$, where δ is the Kronecker delta [3, 19]. Arnault et al. [1] identified the lowest complexity of self-dual normal bases for extensions of low degree and showed that the best complexity of normal bases is often achieved from a self-dual normal basis. In [22, 4.2], Vinatier considered cyclotomic extensions of the rationals generated by d^2-th roots of unity, where d is a prime. The construction they used yields a candidate for the lowest complexity basis for $\mathbb{F}_{p^d}/\mathbb{F}_p$, where $p \neq d$ is a prime which does not split in the chosen extension. They proved that the multiplication table of this basis can be geometrically interpreted by means of an appropriate minimal Besicovitch arrangement. The complexity of the basis, denoted by C_d, is here equal to the number of all but the simple points generated by this arrangement in ${\mathbb{F}_d}^2$ [22].

After a brief overview of the properties of this arrangement, we compare the complexity C_d with the expected value of the number of all but the simple points in a minimal randomly selected Besicovitch arrangement in ${\mathbb{F}_d}^2$ for the first 370 prime numbers d. The expectations are determined using Blondeau Da Silva's results in [5]. In a third part, we consider particular minimal Besicovitch arrangements which share several geometrical properties with the arrangements considered to determine the complexity. We compare again, in this part, for the first 370 prime numbers d, C_d with the expected value of the number of all but the simple points in the randomly selected mentioned above arrangement.

2. The minimal Besicovitch arrangement providing the complexity of the basis

Let d be a prime number and $\mathbb{F}_d$ be the d elements finite field.

A line, in ${\mathbb{F}_d}^2$, is a one-dimensional affine subspace. A Besicovitch arrangement B is a set of lines that contains at least one line in each direction. A minimal Besicovitch arrangement is a Besicovitch arrangement that is the union of exactly $d+1$ lines in ${\mathbb{F}_d}^2$ (see [4] and [5]).

The minimal Besicovitch arrangement considered, brought out by Vinatier [22], and denoted by $\mathscr{L}$, is composed of $d+1$ lines with the equations

$$\begin{cases} L_a: & ax-(a+1)y-p(a)=0, \quad a \in \mathbb{F}_d, \\ L_\infty: & x-y=0, \end{cases}$$

where p is the polynomial

$$p(x) = \frac{(x+1)^d - x^d - 1}{d}, \quad x \in \mathbb{F}_d. \tag{1}$$

For $d \geq 5$, Vinatier [22] proved that under the action of $\Gamma = \langle \iota, \theta \rangle$ (a group generated by two elements of $GL_2(\mathbb{F}_d)$, where $\iota(x,y) = (y,x)$ and $\theta(x,y) = (y-x,-x)$ for $(x,y) \in {\mathbb{F}_d}^2$), this arrangement $\mathscr{L}$ always has two orbits of cardinality 3: $\{L_0, L_{-1}, L_\infty\}$ and $\{L_1, L_{\frac{d-1}{2}}, L_{-2}\}$. They also stated that:

- if $d \equiv 1 \pmod 3$, then there is one orbit $\{L_\omega, L_{\omega^2}\}$ of cardinality 2, where ω is a primitive cubic root of unity in $\mathbb{F}_d$, and the number of orbits of cardinality 6 is $(d-7)/6$;
- if $d \equiv 2 \pmod 3$, then the number of orbits of cardinality 6 is $(d-5)/6$.

The Comp_lib 1.1 package was implemented in Python 3.4. It provides the complexity C_d of the basis (by counting all but the simple points in the associated minimal Besicovitch arrangement, see [22]) and it also enables to determine the points multiplicities distribution in ${\mathbb{F}_d}^2$ of this arrangement. It is available at `https://pypi.python.org/pypi/Comp_lib/1.1`. Table 1 in Appendix gathers the first 370 values of C_d.

3. Complexity versus number of all but simple points in randomly selected arrangements

Let us denote by A_d the expected value of the number of all but the simple points in a randomly chosen minimal Besicovitch arrangement in ${\mathbb{F}_d}^2$. Thanks to the proof of Theorem 1 in [5], we have

$$\begin{aligned} A_d &= d^2 - d\,(d+1)\left(1-\frac{1}{d}\right)^d \\ &= \left(1-\frac{1}{e}\right)d^2 - \frac{1}{2e}d + O\left(1\right), \quad \text{as } d \to \infty. \end{aligned}$$

Figure 1 shows the values of $(C_d - A_d)/d$ for the first 370 prime numbers.

3.1. A first test. From the 370 values of Figure 1, we plot the regression line: its slope s is approximately 4.94×10^{-5} and its intercept is approximately -0.913.

Let us consider the following null hypothesis H_0: $s = 0$. We have to calculate $T = (s-0)/\hat{\sigma}_s$, where $\hat{\sigma}_s$ is the estimated standard deviation of the slope. We obtain $\hat{\sigma}_s \approx 8.74 \times 10^{-5}$ and $T \approx 0.565$. This latter statistic follows a Student's t-distribution with $(370-2)$ degrees of freedom (see [7, Proposition 1.8]). The acceptance region of the hypothesis test with a 5% risk is approximately $[-1.967, 1.967]$. Thus it can be concluded that we cannot reject the null hypothesis: the fact that the slope is not significantly different from zero can not be rejected.

3.2. A second test. Figure 2 below shows the distribution of the values of $(C_d - A_d)/d$ for the first 370 prime numbers. In regard to the resulting histogram, one may wonder whether these values are normally distributed or not.

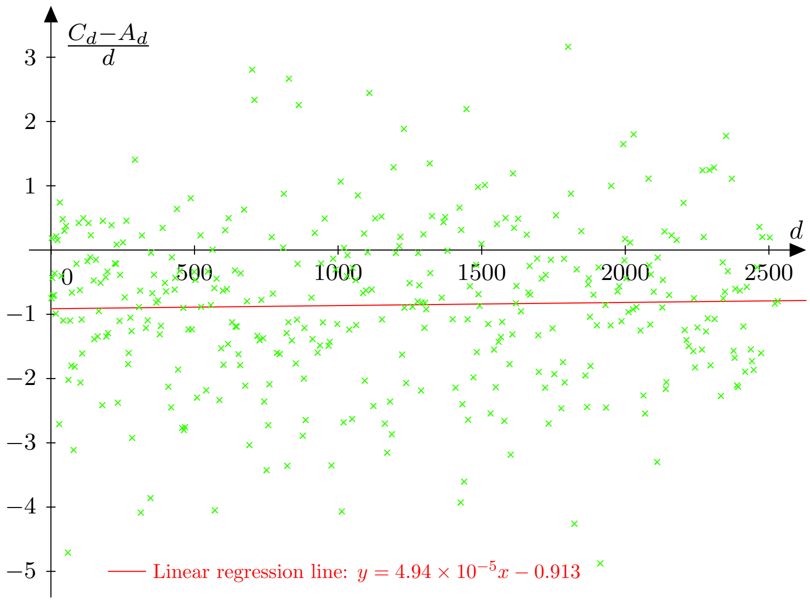

FIGURE 1. The 370 values of the function that relates each prime number d to $\frac{C_d - A_d}{d}$.

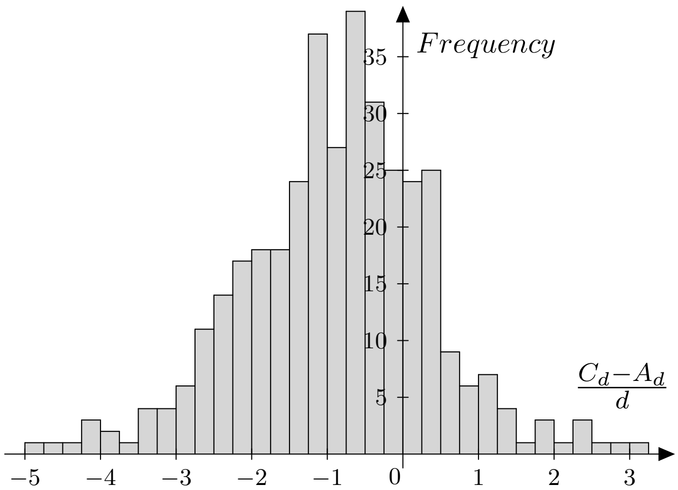

FIGURE 2. Distribution of the values of $\frac{C_d - A_d}{d}$.

From the result of the first test, we would consider in this part that the function that maps d onto $(C_d - A_d)/d$ behaves like a random variable with an expected value Λ close to -0.856. On that assumption we verify whether the values of $(C_d - A_d)/d$ are normally distributed for $d \in [2, 2531] \cap \mathbb{N}$ (the null hypothesis) or not. For this purpose we use the Shapiro–Wilk test (see [20]). The test statistic W is about 0.991. The associated p-value being about 0.0296, it can be concluded that we can reject the null hypothesis, i.e., the values of $(C_d - A_d)/d$ are significantly not normally distributed for $d \in [2, 2531] \cap \mathbb{N}$.

3.3. A third set of tests. Once more, from the result of the first test, we would consider in this part that the function that maps d onto $(C_d - A_d)/d$ behaves like a random variable with an expected value Λ close to -0.856 and with a symmetric probability distribution.

On that assumption we verify whether the values higher than Λ and those smaller than Λ are randomly scattered over the ordered absolute values of $(C_d - A_d)/d$ (the null hypothesis) or not. To this end we use a non-parametric test, the Mann–Whitney U test: we determine the ranks of $|(C_d - A_d)/d|$ for each d in the considered interval (see [15], [24] or more recents books with applications [11, 13]). The ranks sum of the values higher than Λ is approximately normally distributed. The value of U_1 is about -0.911. The acceptance region of the hypothesis test with a 5% risk being approximately $[-1.960, 1.960]$, it can be concluded that we cannot reject the null hypothesis, i.e., the fact that the greater and smaller than Λ values of $(C_d - A_d)/d$ for $d \in [2, 2531] \cap \mathbb{N}$ are randomly scattered: the symmetry of the probability distribution of our potential pseudorandom variable can not be rejected.

Once more, on our first assumption, we verify whether the values higher than Λ and those smaller than Λ are randomly scattered over the first 370 prime numbers (the null hypothesis) or not. To this end we use the same test, the Mann–Whitney U test. The prime number ranks sum of the values higher than Λ is approximately normally distributed. The value of U_2 is about -0.397. It can be concluded that we cannot reject the null hypothesis, i.e., the fact that the greater or smaller than Λ values of $(C_d - A_d)/d$ for $d \in [2, 2531] \cap \mathbb{N}$ are randomly scattered over the first 370 prime numbers.

3.4. Perspective. Both first test and set of tests could not invalidate the fact that the function that maps d onto $(C_d - A_d)/d$ seems to behave like a random variable with Λ as expected value. If we succeed in proving such a statement, we could consider the following unbiased estimator of C_d, denoted by $\widehat{C_d}$:

$$\begin{aligned} \widehat{C_d} &= A_d + \Lambda d \\ &= d^2 - d\,(d+1)\left(1 - \frac{1}{d}\right)^d + \Lambda d \\ &= \left(1 - \frac{1}{e}\right) d^2 + \left(\Lambda - \frac{1}{2e}\right) d + o(d), \quad \text{as } d \to \infty, \end{aligned}$$

thanks to the proof of [5, Theorem 1].

4. Complexity versus number of all but simple points in particular arrangements

4.1. Further details on the minimal Besicovitch arrangements providing the complexity of the normal bases. In this part, we consider particular minimal Besicovitch arrangements which share several geometrical properties with the arrangements considered to determine the complexity, and we compare the expected values of the number of all but simple points in such randomly selected arrangements with C_d values.

Before reviewing the whole cycles highlighted in Section 2, let us make a quick remark.

Remark 4.1. If a line in an orbit passes through $(0,0) \in {\mathbb{F}_d}^2$ all the other lines of this orbit also pass through this point, the elements of the group Γ acting on the lines being in $GL_2(\mathbb{F}_d)$.

In Section 2 two cases appear, for $d \geq 5$: the cases where $d \equiv 1 \pmod 3$ and those where $d \equiv 2 \pmod 3$.

In both cases, the intercepts of the lines in $\{L_0, L_{-1}, L_\infty\}$ are 0 (we have $p(0) = 0$ thanks to equality (1), Remark 4.1 allowing us to conclude).

The intercepts of the lines in $\{L_1, L_{\frac{d-1}{2}}, L_{-2}\}$ are nonzero values, except for $d = 1093$, the first Wieferich prime number, for which lines intercepts are all zero: $p(2) = 0$ if and only if $(2^{d-1} - 1)/d$ (see equality (1), Remark 4.1, and [8]).

If $d \equiv 1 \pmod 3$, the intercepts of the lines in $\{L_\omega, L_{\omega^2}\}$ are 0:

$$p(\omega) = \frac{(\omega+1)^d - \omega^d - 1}{d} = \frac{-\left(\omega^d\right)^2 - \omega^d - 1}{d} = -\frac{-(\omega)^2 - \omega - 1}{d} = 0,$$

using the fact that ω is a primitive cubic root of unity in $\mathbb{F}_d$, and using Fermat's little theorem.

In this part, we only consider the values of $d \in [2, 2531] \cap \mathbb{N}$ where all lines in the 6-cycles do not pass through $(0,0)$; for the 152 values of d verifying this constraint and also $d \equiv 1 \pmod 3$. We denote by M_d^* the expected value of the number of all but the simple points in a randomly chosen arrangement sharing geometrical properties with the arrangement providing the complexity; for the 153 values of d verifying the same constraint and also $d \equiv 2 \pmod 3$, we denote by M_d^{**} the similar expected value. Table 1, in Appendix, shows the values of d being in either the first or the second case.

4.2. Lines intersections of the different cycles. The five functions in Γ, other than the identity function Id, are denoted, for $(x,y) \in {\mathbb{F}_d}^2$, as in [22]:

$$\iota(x,y) = (y,x), \qquad \theta(x,y) = (y-x,-x), \qquad \theta^2(x,y) = (-y, x-y),$$

$$\kappa(x,y) = \theta \circ \iota(x,y) = (x-y,-y), \qquad \lambda(x,y) = \iota \circ \theta(x,y) = (-x, y-x).$$

Note that ι, κ and λ are of order 2, and θ and θ^2 are of order 3. We can also easily verify that the fixed points of ι are those of the line L_∞, the fixed points of κ are those of the line L_0 and the fixed points of λ are those of the line L_{-1}. The following proposition can thus be proved.

Proposition 4.2. *For all $\gamma \in \{\iota, \kappa, \lambda\}$ and for all $a \in \mathbb{F}_d \setminus \{0,-1\}$, if L_a and $\gamma(L_a)$ are two distinct lines, then their intersection point is in line of the fixed points of γ.*

Proof. The image of a point under a function in $\Gamma \subset GL_2(\mathbb{F}_d)$ is a point. So, for all $\gamma \in \{\iota, \kappa, \lambda\}$ and for all $a \in \mathbb{F}_d \setminus \{0,-1\}$, if L_a and $\gamma(L_a)$ are two distinct lines, i.e., if their intersection is a point:

$$\gamma\left(L_a \cap \gamma(L_a)\right) = \gamma(L_a) \cap \gamma\left(\gamma(L_a)\right) = L_a \cap \gamma(L_a),$$

each of the considered functions being of order 2. The point $L_a \cap \gamma(L_a)$ is thus in the fixed line of γ. □

Let us henceforth denote by $\mathscr{T}$ the set ${\mathbb{F}_d}^2 \setminus \{L_0, L_{-1}, L_\infty\}$. In each 6-cycle, for all $\gamma \in \Gamma$ and for all $a \in \mathbb{F}_d$ (such that L_a is in the considered 6-cycle), L_a and $\gamma(L_a)$ are distinct; we can therefore apply Proposition 4.2: in the case where all the lines in a 6-cycle do not pass through $(0,0)$ (the prevalent selected case in Subsection 4.1), there exist 3 intersection points of the 6-cycle lines on each line of $\{L_0, L_{-1}, L_\infty\}$:

- on L_0: $L_a \cap \kappa(L_a)$, $\theta(L_a) \cap \lambda(L_a)$ and $\theta^2(L_a) \cap \iota(L_a)$;
- on L_{-1}: $L_a \cap \lambda(L_a)$, $\theta(L_a) \cap \iota(L_a)$ and $\theta^2(L_a) \cap \kappa(L_a)$;
- on L_∞: $L_a \cap \iota(L_a)$, $\theta(L_a) \cap \kappa(L_a)$ and $\theta^2(L_a) \cap \lambda(L_a)$.

We have the following proposition.

Proposition 4.3. *In the case where all the lines in a 6-cycle do not pass through $(0,0)$, two of the described above 6-cycle intersection points on a line of $\{L_0, L_{-1}, L_\infty\}$ do not coincide.*

Proof. Let us consider a 6-cycle. Its lines do not pass through the origin. Let $a \in \mathbb{F}_d$, such that L_a is in this 6-cycle. We assume that $L_a \cap \kappa(L_a)$ and $\theta(L_a) \cap \lambda(L_a)$ coincide on L_0. Knowing that $\theta(L_0) = L_\infty$ (see [22]), we have

$$\theta(L_a \cap \kappa(L_a) \cap \theta(L_a) \cap \lambda(L_a)) \in L_\infty,$$
$$\theta(L_a) \cap \lambda(L_a) \cap \theta^2(L_a) \cap \iota(L_a) \in L_\infty.$$

So $\theta(L_a) \cap \lambda \in L_0 \cap L_\infty = (0,0)$. It contradicts the hypothesis of the proposition. The considered points do not coincide. All the other cases can be demonstrated in the same way. □

Thus the remaining 6 intersection points of the 6-cycle lines are in $\mathscr{T}$. We can finally prove the following proposition (in the case where $d \geq 11$, otherwise there is no 6-cycle in the arrangement $\mathscr{L}$).

Proposition 4.4. *The* 6 *remaining points in* $\mathscr{T}$ *(in the case where all the lines in the* 6*-cycle do not pass through* $(0,0)$*) are distinct.*

Proof. We first prove the following lemma.

Lemma 4.5. θ *has a single fixed point in* ${\mathbb{F}_d}^2$ *if and only if* $d \neq 3$.

Proof. Let $\theta \in GL_2(\mathbb{F}_d)$. Then $(0,0)$ is a fixed point of θ. For $(x,y) \in {\mathbb{F}_d}^2$:

$$\begin{aligned} \theta(x,y) = (x,y) \quad & \text{if and only if} \quad y - x = x \text{ and } -x = y \\ & \text{if and only if} \quad 3x = 0 \text{ and } y = -x. \end{aligned}$$

The result follows. ☐

Now, let us consider a 6-cycle. Its lines do not pass through the origin. Let $a \in \mathbb{F}_d$, such that L_a is in this 6-cycle. Assume that 3 lines in the 6-cycle are concurrent in $P \in \mathscr{T}$. It is clear from the foregoing that these lines are whether L_a, $\theta(L_a)$ and $\theta^2(L_a)$ or $\iota(L_a)$, $\kappa(L_a)$ and $\lambda(L_a)$. We have

$$\begin{aligned} \theta(P) &= \theta\left(L_a \cap \theta(L_a) \cap \theta^2(L_a)\right) \quad (\text{or} \quad \theta\left(\iota(L_a) \cap \kappa(L_a) \cap \lambda(L_a)\right)) \\ &= \theta(L_a) \cap \theta^2(L_a) \cap L_a \quad (\text{or} \quad \kappa(L_a) \cap \lambda(L_a) \cap \iota(L_a)). \end{aligned}$$

In both cases $\theta(P) = P$, i.e., P is a fixed point of θ. It means that $P = (0,0)$ thanks to Lemma 4.5, knowing that $d \geq 11$. This contradicts the hypothesis of the proposition. The 6 remaining points in $\mathscr{T}$ are distinct. ☐

The cases of $\{L_1, L_{\frac{d-1}{2}}, L_{-2}\}$ and $\{L_\omega, L_{\omega^2}\}$ can be considered as degenerate cases of a 6-cycle. Let us focus on the first arrangement. From [22], we get $\iota(L_1) = L_{-2}$, $\lambda(L_{-2}) = L_{\frac{d-1}{2}}$ and $\kappa(L_1) = L_{\frac{d-1}{2}}$. Thanks to Proposition 4.2, the 3 intersection points of lines in $\{L_1, L_{\frac{d-1}{2}}, L_{-2}\}$ are:

$$L_1 \cap L_{\frac{d-1}{2}} \text{ on } L_0; \quad L_{-2} \cap L_{\frac{d-1}{2}} \text{ on } L_{-1}; \quad L_1 \cap L_{-2} \text{ on } L_\infty.$$

We note that this result is just a particular case of the above result.

Figure 3 below provides two examples of minimal Besicovitch arrangements leading to the determination of the complexity. For the first one ($d = 7$), we are in the case where $d \equiv 1 \pmod 3$, for the second one ($d = 11$) in the case where $d \equiv 2 \pmod 3$. The above results and in particular those of Propositions 4.2, 4.3 and 4.4 are emphasised.

4.3. The first model. We first consider the case where $d \equiv 1 \pmod 3$. Let us denote by Ω^* the set of minimal Besicovitch arrangements verifying some geometrical constraints similar to those of the considered Besicovitch arrangements. In such arrangements:

- there exist 3 lines of equations $x = 0$, $y = 0$ and $y = x$ (let us denote by l_a this lines set);
- there exist 2 lines that pass through the origin (let us denote by l_2 this lines set);

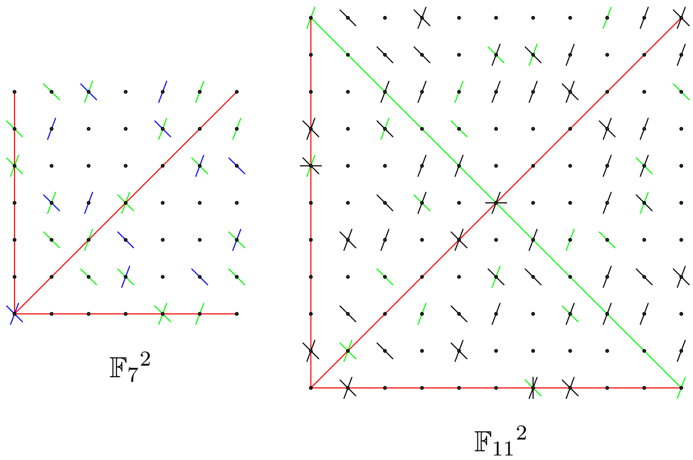

FIGURE 3. Lines of the minimal Besicovitch arrangement in $\mathbb{F}_d{}^2$ providing the complexity C_d where $d = 7$ (on the left) and $d = 11$ (on the right). The number of all but the simple points is 25 for $d = 7$, and 67 for $d = 11$; thus $C_7 = 25$ and $C_{11} = 67$.

- there exist 3 lines that do not pass through the origin, their 3 intersection points being respectively on each of the 3 lines in l_a (let us denote by l_3 this lines set);
- there exist $(d-7)/6$ sets of 6 lines, all verifying the same constraints as in Propositions 4.2, 4.3 and 4.4.

In order to calculate the average number of all but simple points in such arrangements, we build a probability space: Ω^*. The σ-algebra chosen here is the finite collection of all subsets of Ω^*. Our probability measure, denoted by P, assigns equal probabilities to all outcomes.

For Q in $\mathbb{F}_d{}^2$, let M_Q be the random variable that maps $A \in \Omega^*$ to the multiplicity of Q in A.

With the aim of knowing the expected number of simple points in such particular arrangements, we determine $\mathrm{P}(M_Q = 1)$, for all Q in $\mathbb{F}_d{}^2$. Two cases appear: either Q is in a line of l_a (apart from the origin) or not.

4.3.1. *Q is in a line of l_a (apart from the origin).* In this case, for $A \in \Omega^*$, we have:

$$M_Q(A) = 1 \text{ if and only if none of the } d-2 \text{ lines of } A \text{ (other than those of } l_a) \text{ pass through } Q.$$

We already know that lines of l_2 do not pass through this point.

There is a $\frac{d-2}{d-1} \times \frac{d-3}{d-2}$ probability that the two distinct intersection points between lines of l_3 and the considered line of l_a do not coincide with Q (a line is composed of d points and the origin is here not considered).

Similarly, there is a $\frac{d-2}{d-1} \times \frac{d-3}{d-2} \times \frac{d-4}{d-3}$ probability that the three distinct intersection points between lines of a set of 6 lines (verifying the same constraints as in Propositions 4.2 and 4.3) and the considered line of l_a do not coincide with Q.

Finally, considering the $(d-7)/6$ sets of 6 lines and the lines in l_2 and l_3, we obtain

$$\mathrm{P}\left(M_Q = 1\right) = \frac{d-3}{d-1} \times \left(\frac{d-4}{d-1}\right)^{\frac{d-7}{6}}.$$

4.3.2. *Q is not in a line of l_a.* In this case, for $A \in \Omega^*$, we have:

$M_Q(A) = 1$ if and only if exactly one line of the $d-2$ lines of A (other than those of l_a) passes through Q.

We use the following results to study in more detail the different subcases. In ${\mathbb{F}_d}^2 \backslash l_a$, there are $d^2 - 3 \times (d-1) - 1 = d^2 - 3d + 2$ points. In ${\mathbb{F}_d}^2 \backslash l_a \cup l_2$, there are $2(d-1)$ points of multiplicity 1 and the remaining points of multiplicity 0 ($d^2 - 5d + 4$ points). In ${\mathbb{F}_d}^2 \backslash l_a \cup l_3$, there are $3(d-3)$ points of multiplicity 1 and the remaining points of multiplicity 0 ($d^2 - 6d + 11$ points). In the union of ${\mathbb{F}_d}^2 \backslash l_a$ and a 6 lines set, there are $6(d-5)$ points of multiplicity 1, 6 points of multiplicity 2 (see Proposition 4.4) and the remaining points of multiplicity 0 ($d^2 - 9d + 26$ points).

This case can be divided into 3 subcases:

- the first one where the line that passes through Q is in l_2; then the probability is

$$\frac{2(d-1)}{d^2-3d+2} \times \frac{d^2-6d+11}{d^2-3d+2} \times \left(\frac{d^2-9d+26}{d^2-3d+2}\right)^{\frac{d-7}{6}};$$

- the second one where the line that passes through Q is in l_3; then the probability is

$$\frac{d^2-5d+4}{d^2-3d+2} \times \frac{3(d-3)}{d^2-3d+2} \times \left(\frac{d^2-9d+26}{d^2-3d+2}\right)^{\frac{d-7}{6}};$$

- the third one where the line that passes through Q is in one of the $\frac{d-7}{6}$ sets of 6 lines; then the probability is

$$\frac{d^2-5d+4}{d^2-3d+2} \times \frac{d^2-6d+11}{d^2-3d+2} \times \frac{d-7}{6} \frac{6(d-5)}{d^2-3d+2} \left(\frac{d^2-9d+26}{d^2-3d+2}\right)^{\frac{d-13}{6}}.$$

Hence, in this specific case we have that

$$\begin{aligned}
\mathrm{P}\left(M_Q=1\right)=&\frac{2}{d-2}\times\frac{d^2-6d+11}{d^2-3d+2}\times\left(\frac{d^2-9d+26}{d^2-3d+2}\right)^{\frac{d-7}{6}}\\
&+\frac{d-4}{d-2}\times\frac{3(d-3)}{d^2-3d+2}\times\left(\frac{d^2-9d+26}{d^2-3d+2}\right)^{\frac{d-7}{6}}\\
&+\frac{d-4}{d-2}\times\frac{d^2-6d+11}{d^2-3d+2}\times\frac{d^2-12d+35}{d^2-3d+2}\left(\frac{d^2-9d+26}{d^2-3d+2}\right)^{\frac{d-13}{6}}.
\end{aligned}$$

4.3.3. *The expected value of M_d^*.* Recall that our aim is to determine the expected value M_d^* of the number of all but simple points in arrangements of Ω^* in order to compare it with the value of the complexity C_d.

Thanks to the results of the above section and knowing that the first case concerns $3d-3$ points and the second one d^2-3d+2 points, we get

$$\begin{aligned}
M_d^* =&d^2-\left[3(d-3)\times\left(\frac{d-4}{d-1}\right)^{\frac{d-7}{6}}+\frac{2(d^2-6d+11)}{d-2}\left(\frac{d^2-9d+26}{d^2-3d+2}\right)^{\frac{d-7}{6}}\right.\\
&+\frac{3(d-3)(d-4)}{d-2}\times\left(\frac{d^2-9d+26}{d^2-3d+2}\right)^{\frac{d-7}{6}}\\
&\left.+\frac{(d-4)(d^2-6d+11)}{d-2}\times\frac{d^2-12d+35}{d^2-3d+2}\left(\frac{d^2-9d+26}{d^2-3d+2}\right)^{\frac{d-13}{6}}\right].
\end{aligned}$$

Using the Computer Algebra System Giac/Xcas [21], we obtain that

$$M_d^*=\left(1-\frac{1}{e}\right)d^2+\left(\frac{1}{e}-3\exp(-\frac{1}{2})\right)d+O\left(1\right),\quad \text{as } d\to\infty.$$

4.4. The second model. We henceforth consider the case where $d\equiv 2 \pmod 3$. Let us denote by Ω^{**} the set of minimal Besicovitch arrangements verifying some geometrical constraints similar to those of the considered Besicovitch arrangements. In such arrangements:

- there exist 3 lines of equations $x=0$, $y=0$ and $y=x$ (let us denote by l_a this lines set);
- there exist 3 lines that do not pass through the origin, their 3 intersection points being respectively on each of the 3 lines in l_a (let us denote by l_3 this lines set);
- there exist $(d-5)/6$ sets of 6 lines, all verifying the same constraints as in Propositions 4.2, 4.3 and 4.4.

In order to calculate the average number of all but simple points in such arrangements, we build a probability space: Ω^{**}. The σ-algebra chosen here is the finite collection of all subsets of Ω^{**}. Our probability measure, denoted by P, assigns equal probabilities to all outcomes.

For Q in ${\mathbb{F}_d}^2$, let M_Q be the random variable that maps $A \in \Omega^{**}$ to the multiplicity of Q in A.

With the aim of knowing the expected number of simple points in such particular arrangements, we determine $\mathrm{P}\left(M_Q = 1\right)$, for all Q in ${\mathbb{F}_d}^2$. Two cases appear: either Q is in a line of l_a (apart from the origin) or not.

4.4.1. *Q is in a line of l_a (apart from the origin).* In this case, for $A \in \Omega^{**}$, we have:

$M_Q(A) = 1$ if and only if none of the $d-2$ lines of A (other than those of l_a) pass through Q.

There is a $\frac{d-2}{d-1} \times \frac{d-3}{d-2}$ probability that the two distinct intersection points between lines of l_3 and the considered line of l_a do not coincide with Q.

Similarly, there is a $\frac{d-2}{d-1} \times \frac{d-3}{d-2} \times \frac{d-4}{d-3}$ probability that the three distinct intersection points between lines of a set of 6 lines and the considered line of l_a do not coincide with Q.

Finally, considering the $(d-5)/6$ sets of 6 lines and the lines in l_3, we obtain

$$\mathrm{P}\left(M_Q = 1\right) = \frac{d-3}{d-1} \times \left(\frac{d-4}{d-1}\right)^{\frac{d-5}{6}}.$$

4.4.2. *Q is not in a line of l_a.* In this case, for $A \in \Omega^{**}$, we have:

$M_Q(A) = 1$ if and only if exactly one line of the $d-2$ lines of A (other than those of l_a) passes through Q.

We use the following results to study in more detail the different subcases. In ${\mathbb{F}_d}^2 \setminus l_a$, there are $d^2 - 3d + 2$ points. In ${\mathbb{F}_d}^2 \setminus l_a \cup l_3$, there are $3(d-3)$ points of multiplicity 1 and the remaining points of multiplicity 0 ($d^2 - 6d + 11$ points). In the union of ${\mathbb{F}_d}^2 \setminus l_a$ and a 6 lines set, there are $6(d-5)$ points of multiplicity 1, 6 points of multiplicity 2 (see Proposition 4.4) and the remaining points of multiplicity 0 ($d^2 - 9d + 26$ points).

This case can be divided into 2 subcases:

- the first one where the line that passes through Q is in l_3; then the probability is

$$\frac{3(d-3)}{d^2 - 3d + 2} \times \left(\frac{d^2 - 9d + 26}{d^2 - 3d + 2}\right)^{\frac{d-5}{6}};$$

- the second one where the line that passes through Q is in one of the $\frac{d-5}{6}$ sets of 6 lines; then the probability is

$$\frac{d^2 - 6d + 11}{d^2 - 3d + 2} \times \frac{d-5}{6} \frac{6(d-5)}{d^2 - 3d + 2} \left(\frac{d^2 - 9d + 26}{d^2 - 3d + 2}\right)^{\frac{d-11}{6}}.$$

Hence in this specific case we have

$$\begin{aligned}\mathrm{P}\left(M_Q=1\right)=&\frac{3(d-3)}{d^2-3d+2}\times\left(\frac{d^2-9d+26}{d^2-3d+2}\right)^{\frac{d-5}{6}}\\&+\frac{d^2-6d+11}{d^2-3d+2}\times\frac{d^2-10d+25}{d^2-3d+2}\left(\frac{d^2-9d+26}{d^2-3d+2}\right)^{\frac{d-11}{6}}.\end{aligned}$$

4.4.3. *The expected value of M_d^{**}.* Recall that our aim is to determine the expected value M_d^{**} of the number of all but simple points in arrangements of Ω^{**} in order to compare it with the value of the complexity C_d.

Thanks to the results of the above section and knowing that the first case concerns $3d-3$ points and the second one d^2-3d+2 points, we get

$$\begin{aligned}M_d^{**}=&d^2-\Bigg[3(d-3)\times\left(\frac{d-4}{d-1}\right)^{\frac{d-5}{6}}+3(d-3)\times\left(\frac{d^2-9d+26}{d^2-3d+2}\right)^{\frac{d-5}{6}}\\&+(d^2-6d+11)\times\frac{d^2-10d+25}{d^2-3d+2}\left(\frac{d^2-9d+26}{d^2-3d+2}\right)^{\frac{d-11}{6}}\Bigg].\end{aligned}$$

Using the Computer Algebra System Xcas, we obtain that

$$M_d^{**}=\left(1-\frac{1}{e}\right)d^2+\left(\frac{1}{e}-3\exp(-\frac{1}{2})\right)d+O\left(1\right),\quad \text{as } d\to\infty.$$

4.5. Results. Figure 4 shows values of both $(C_d-M_d^*)/d$ and $(C_d-M_d^{**})/d$ for the selected prime numbers d.

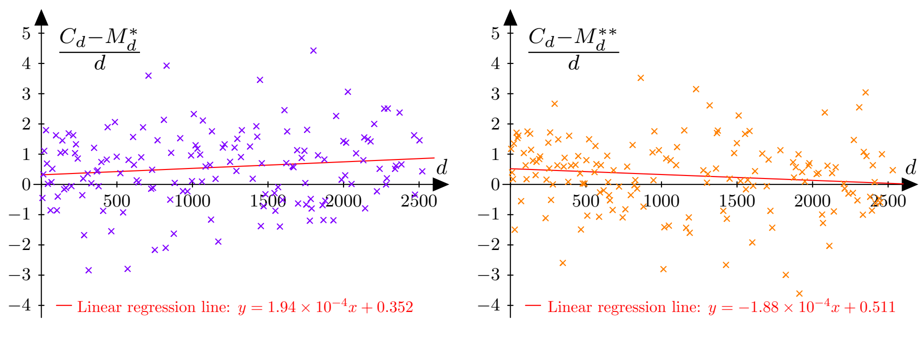

FIGURE 4. Values of both $\frac{C_d-M_d^*}{d}$ (on the left) and $\frac{C_d-M_d^{**}}{d}$ (on the right) for the selected prime numbers d.

4.5.1. *A first test in each case.* From the 152 left plotted values on Figure 4, we draw the regression line: its slope s^* is approximately 1.94×10^{-4} and its intercept is approximately 0.352. Let us consider the following null hypothesis H_0^*: $s^* = 0$. We have to calculate $T^* = (s^* - 0)/\hat{\sigma}_{s^*}$, where $\hat{\sigma}_{s^*}$ is the estimated standard deviation of the slope. We obtain $\hat{\sigma}_{s^*} \approx 1.35 \times 10^{-4}$ and $T^* \approx 1.43$. This latter statistic follows a Student's t-distribution with $(152 - 2)$ degrees of freedom [7, Proposition 1.8]. The acceptance region of the hypothesis test with a 5% risk is approximately $[-1.976, 1.976]$. Thus it can be concluded that we cannot reject the null hypothesis, i.e., the fact that the slope s^* is not significantly different from zero.

From the 153 right plotted values on Figure 4, we draw the regression line: its slope s^{**} is approximately -1.88×10^{-4} and its intercept is approximately 0.511. Let us consider the following null hypothesis H_0^{**}: $s^{**} = 0$. We again have to calculate $T^{**} = (s^{**} - 0)/\hat{\sigma}_{s^{**}}$. We here obtain $\hat{\sigma}_{s^{**}} \approx 1.25 \times 10^{-4}$ and $T^{**} \approx -1.50$. This latter statistic follows a Student's t-distribution with $(153 - 2)$ degrees of freedom. The acceptance region of the hypothesis test with a 5% risk is approximately $[-1.976, 1.976]$. Thus it can be concluded that we cannot reject the fact that the slope s^{**} is not significantly different from zero.

4.5.2. *A set of tests in each case.* Figure 5 below shows the distribution of the values of $C_d - M_d^*/d$ (on the left) and $C_d - M_d^{**}/d$ (on the right) for the considered values of d.

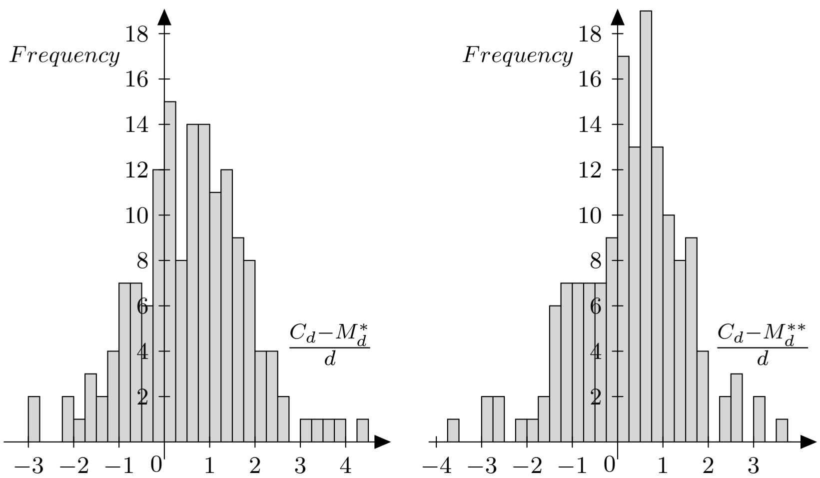

FIGURE 5. Distribution of values of both $\frac{C_d - M_d^*}{d}$ (on the left) and $\frac{C_d - M_d^{**}}{d}$ (on the right) for the selected prime numbers d.

From the result of the first test in Section 4.5.1, we would consider in this part that the function that maps d onto $(C_d - M_d^*)/d$ behaves like a random variable with an expected value Λ^* close to 0.576 and with a symmetric probability distribution (for the considered values of d). On that assumption we verify whether the values higher than Λ^* and those smaller than Λ^* are randomly scattered over the ordered absolute values of $(C_d - A_d)/d$ (the null hypothesis) or not. To this end we use a non-parametric test, the Mann–Whitney U test: we determine the ranks of $|(C_d - M_d^*)/d|$ for each d in the considered interval (see [15] or [24]). The ranks sum of the values higher than Λ^* is approximately normally distributed. The value of U_1^* is about -0.673. The acceptance region of the hypothesis test with a 5% risk being approximately $[-1.960, 1.960]$, it can be concluded that we cannot reject the null hypothesis, i.e., the fact that the greater or smaller than Λ^* values of $(C_d - M_d^*)/d$ are randomly scattered: the symmetry of the probability distribution of this potential pseudorandom variable can not be rejected.

On the same assumption, we also verify whether the values higher or smaller than Λ^* are randomly scattered over the considered prime numbers (the null hypothesis) or not. To this end we again use the Mann–Whitney U test. The prime numbers ranks sum of the values higher than Λ^* is approximately normally distributed. The value of U_2^* is about 0.721. It can be concluded that we cannot reject the null hypothesis, i.e., the fact that the greater or smaller than Λ^* values of $(C_d - M_d^*)/d$ are randomly scattered over the considered prime numbers.

From the result of the second test in 4.5.1, we would consider in this part that the function that maps d onto $(C_d - M_d^{**})/d$ behaves like a random variable with an expected value Λ^{**} close to 0.297 and with a symmetric probability distribution (for the considered values of d). On that assumption we verify whether the values higher than Λ^{**} and those smaller than Λ^{**} are randomly scattered over the ordered absolute values of $(C_d - A_d)/d$ (the null hypothesis) or not. To this end we again use the Mann–Whitney U test. The value of U_1^{**} is here about -1.08. It can once more be concluded that we cannot reject the fact that the greater or smaller than Λ^{**} values of $(C_d - M_d^{**})/d$ are randomly scattered: the symmetry of the probability distribution of this potential pseudorandom variable can not be rejected.

On the same assumption, we verify whether the values higher than Λ^{**} and those smaller than Λ^{**} are randomly scattered over the considered prime numbers or not. To this end we again use the Mann–Whitney U test. The value of U_2^{**} is here about -1.77. It can once more be concluded that we cannot reject the fact that the greater or smaller than Λ^{**} values of $(C_d - M_d^{**})/d$ are randomly scattered over the considered prime numbers.

4.5.3. *Perspective.* Both first test and set of tests could not invalidate the fact that the function that maps d onto $(C_d - M_d^*)/d$ and the one that maps

d onto $(C_d - M_d^{**})/d$ seem to behave like random variables with respectively Λ^* and Λ^{**} as expected values. Λ^* and Λ^{**} are both positive numbers, whereas Λ is negative; the added geometrical constraints seem to reduce in average the number of all but the simple points generated by a randomly chosen minimal Besicovitch arrangement. This reduction is slightly highter than expected. Our arrangements cannot obviously be limited to the considered geometrically constrained arrangement. Adding constraints for better modeling the arrangements and finding a way to determine whether the considered functions could be considered as high-quality pseudo-random number generators (PRNG) sketch some avenues for future research on the subject.

Appendix

TABLE 1. The complexities values. Values of d with one asterisk correspond to arrangements where $d \equiv 1 \pmod 3$ and where all the lines (except those of $\{L_0, L_{-1}, L_\infty\}$ and $\{L_\omega, L_{\omega^2}\}$) do not pass through the origin, whereas values of d with two asterisks correspond to arrangements where $d \equiv 2 \pmod 3$ and where all the lines (except those of $\{L_0, L_{-1}, L_\infty\}$) do not pass through the origin. In the latter case, when the asterisk is missing, all the lines in some 6-cycle pass through the origin.

d	2	3	5^{**}	7^*	11^{**}	13^*	17^{**}	19^*	23^{**}	29^{**}	31^*	37^*	41^{**}	43^*	47^{**}	53^{**}	59	61^*	67^*	71^{**}
C_d	1	6	13	25	67	100	163	229	334	448	625	844	1075	1114	1402	1786	1912	2218	2752	3046

d	73^*	79	83	89^{**}	97^*	101^{**}	103^*	107^{**}	109^*	113^{**}	127^*	131^{**}	137^{**}	139^*	149^{**}
C_d	3307	3685	4189	4972	5971	6367	6475	7102	7315	8107	10150	10879	11824	12220	13936

d	151^*	157^*	163^*	167^{**}	173^{**}	179	181^*	191^{**}	193	197^{**}	199^*	211^*	223^*
C_d	14176	15529	16546	17440	18799	19789	20758	22945	23251	24430	24739	28186	31348

d	227	229^*	233^{**}	239^{**}	241^*	251^{**}	257^{**}	263^{**}	269^{**}	271^*	277^*	281^{**}	283^*	293^{**}
C_d	32482	33127	33721	35800	36577	39808	41515	43795	45214	45940	48160	49507	49747	54625

d	307^*	311^{**}	313^*	317^{**}	331^*	337	347^{**}	349^*	353^{**}	359^{**}	367^*	373^*	379^*
C_d	59248	60886	60592	63535	68794	71359	74710	76915	78466	81265	84772	87586	90232

d	383^{**}	389^{**}	397^*	401^{**}	409^*	419	421	431^{**}	433^*	439^*	443	449^{**}
C_d	92203	95716	99352	101314	104797	109873	111913	117079	118249	122023	123148	127207

d	457	461^{**}	463^*	467^{**}	479^{**}	487^*	491^{**}	499^*	503^{**}	509^{**}	521^{**}	523^*
C_d	130669	133840	134125	136486	144355	150223	151696	157138	159607	162508	171607	172345

d	541^*	547	557^{**}	563^{**}	569^{**}	571^*	577^*	587^{**}	593^{**}	599^{**}	601	607^*
C_d	183730	188854	195535	200263	204214	203680	210088	216331	221269	226318	227140	232981

d	613^{*}	617^{**}	619	631^{*}	641^{**}	643^{*}	647^{**}	653^{**}	659^{**}	661^{*}	673^{*}	677^{**}
C_d	237046	239626	242398	250861	259405	260467	263722	268363	273217	275827	286606	288166

d	683^{**}	691	701	709^{*}	719^{**}	727^{*}	733^{*}	739^{*}	743^{**}	751^{*}	757	761^{**}
C_d	294208	299602	312463	319282	325690	332941	338929	344065	347074	353806	360034	364345

d	769^{*}	773^{**}	787	797^{**}	809^{**}	811^{*}	821^{**}	823^{*}	827^{**}	829^{*}	839^{**}	853^{*}
C_d	373825	377044	390112	400093	413593	416320	424864	425239	431245	436477	443629	458275

d	857	859^{*}	863^{**}	877^{*}	881^{**}	883^{*}	887	907	911	919^{*}	929	937^{*}
C_d	463174	466087	472573	483487	488704	491626	494824	519175	523180	533941	543892	553420

d	941^{**}	947^{**}	953^{**}	967^{*}	971	977	983^{**}	991^{*}	997^{*}	1009^{*}	1013^{**}	1019^{**}
C_d	559363	565651	574390	589471	594424	599923	610498	620311	627001	644440	644356	653449

d	1021^{*}	1031^{**}	1033^{*}	1039	1049^{**}	1051^{*}	1061^{**}	1063^{*}	1069^{*}	1087^{*}	1091	1093
C_d	658795	671311	674257	680911	692635	697756	710902	712840	723076	745966	752482	752740

d	1097^{**}	1103^{**}	1109	1117^{*}	1123^{*}	1129^{*}	1151^{**}	1153^{*}	1163^{**}	1171^{*}	1181^{**}	1187^{**}
C_d	759808	768805	779941	787798	794254	806077	837823	838891	851632	862882	878656	887017

d	1193	1201^{*}	1213^{*}	1217	1223	1229^{**}	1231	1237	1249^{*}	1259	1277^{**}
C_d	900982	911497	929935	936253	943267	956872	956560	964465	985237	1000621	1029562

d	1279^{*}	1283	1289	1291^{*}	1297^{*}	1301^{**}	1303	1307^{**}	1319^{**}	1321^{*}
C_d	1033756	1039588	1047226	1052251	1063438	1068115	1071913	1078375	1101274	1102360

d	1327^{*}	1361^{**}	1367^{**}	1373^{**}	1381^{*}	1399^{*}	1409^{**}	1423^{*}	1427^{**}	1429^{*}
C_d	1113577	1169632	1181578	1192081	1205287	1235425	1251661	1280677	1281337	1291003

d	1433^{**}	1439	1447^{*}	1451^{**}	1453^{*}	1459^{*}	1471^{*}	1481^{**}	1483^{*}	1487
C_d	1294351	1303495	1326448	1329037	1330435	1344493	1364623	1385854	1387588	1398910

d	1489	1493	1499^{**}	1511^{**}	1523^{**}	1531	1543^{*}	1549^{*}	1553^{**}	1559^{**}
C_d	1400191	1407457	1420246	1444459	1464190	1477492	1502308	1513120	1524895	1533844

d	1567^{*}	1571^{**}	1579^{*}	1583^{**}	1597^{*}	1601^{**}	1607^{**}	1609^{*}	1613	1619^{**}
C_d	1549756	1558054	1571542	1584523	1609036	1614859	1630015	1638106	1644892	1655251

d	1621^{*}	1627^{*}	1637	1657	1663^{*}	1667^{**}	1669^{*}	1693^{*}	1697^{**}	1699^{*}
C_d	1659781	1673800	1692076	1735675	1746766	1755874	1759345	1811281	1817827	1821148

d	1709^{**}	1721^{**}	1723^{*}	1733^{**}	1741^{*}	1747^{*}	1753^{*}	1759^{*}	1777^{*}	1783^{*}
C_d	1845148	1868239	1875610	1893445	1915426	1926787	1938808	1956460	1991359	2006128

d	1787^{**}	1789^{*}	1801^{*}	1811	1823^{**}	1831^{*}	1847	1861^{*}	1867^{*}	1871^{**}
C_d	2018023	2019100	2055712	2074435	2092648	2118334	2156626	2185264	2198473	2211484

d	1873^{*}	1877^{**}	1879^{*}	1889^{**}	1901	1907^{**}	1913^{**}	1931^{**}	1933^{*}	1949^{**}
C_d	2216392	2224747	2228053	2253946	2281783	2297935	2303611	2355019	2356819	2398531

d	1951^{*}	1973^{**}	1979^{**}	1987^{*}	1993	1997	1999^{*}	2003	2011^{*}	2017^{*}
C_d	2407693	2459041	2474182	2493151	2513734	2520214	2525929	2534818	2554063	2571514

d	2027^{**}	2029^{*}	2039^{**}	2053^{*}	2063^{**}	2069^{**}	2081^{**}	2083^{*}	2087	2089
C_d	2594968	2605618	2625871	2661322	2685235	2700313	2739367	2741827	2750443	2757349

d	2099^{**}	2111^{**}	2113	2129^{**}	2131^{*}	2137^{*}	2141^{**}	2143^{*}	2153^{**}	2161^{*}
C_d	2783251	2809579	2821639	2862883	2869180	2886973	2892547	2898181	2928235	2952049

d	2179^{*}	2203^{*}	2207^{**}	2213^{**}	2221^{*}	2237^{**}	2239^{*}	2243	2251	2267^{**}
C_d	3001276	3069025	3075811	3092218	3114424	3159310	3166807	3175720	3199828	3244723

d	2269^{*}	2273^{**}	2281^{*}	2287^{*}	2293^{*}	2297^{**}	2309^{**}	2311	2333^{**}	2339^{**}
C_d	3256783	3265912	3285589	3303373	3326029	3330658	3372679	3373075	3434839	3457402

d	2341^{*}	2347^{*}	2351^{**}	2357^{**}	2371^{*}	2377	2381^{**}	2383^{*}	2389	2393^{**}
C_d	3462010	3480025	3497599	3510505	3555751	3567400	3579163	3587740	3602248	3614269

d	2399^{**}	2411^{**}	2417^{**}	2423	2437	2441^{**}	2447^{**}	2459^{**}	2467^{*}	2473^{*}
C_d	3636025	3671155	3687757	3709300	3749929	3761812	3780007	3821119	3847576	3861457

d	2477	2503^{*}	2521^{*}	2531^{**}
C_d	3878440	3960268	4014841	4046863

References

[1] F. Arnault, E. J. Pickett, and S. Vinatier, *Construction of self-dual normal bases and their complexity*, Finite Fields Appl. **18** (2012), 458–472.

[2] D. W. Ash, I. F. Blake, and S. A. Vanstone, *Low complexity normal bases*, Discrete Appl. Math. **25**(3) (1989), 191–210.

[3] T. Beth, and W. Geiselmann, *Selbstduale Normalbasen über GF(q)*, Arch. Math. (Basel) **55**(1) (1990), 44–48.

[4] S. Blondeau Da Silva, *On minimal Besicovitch arrangements in $\mathbb{F}_q^2$: statistical properties and combinatorial implications*, Bull. Iranian Math. Soc. (2019).

[5] S. Blondeau Da Silva, *On randomly chosen arrangements of $q+1$ lines with different slopes in $\mathbb{F}_q^2$*, J. Number Theory **180** (2017), 533–543.

[6] M. Christopoulou, T. Garefalakis, D. Panario, and D. Thomson, *The trace of an optimal normal element and low complexity normal bases*, Des. Codes Cryptogr. **49**(1-3) (2008), 199–215.

[7] P. A. Cornillon and E. Matzner-Lober, *Régression : Théorie et Applications*, Springer, New York, 2007.

[8] F. G. Dorais and D. Klyve, *A Wieferich prime search up to* 6.7×10^{15}, J. Integer Seq. **14**(9) (2011).

[9] S. Gao, *Normal Bases over Finite Fields*, PhD in Combinatorics and Optimisation, University of Waterloo, Canada, 1993.

[10] S. Gao and H. W. Lenstra Jr., *Optimal normal bases*, Des. Codes Cryptogr. **2**(4) (1992), 315–323.

[11] T. P. Hettmansperger and J. W. McKean, *Robust Nonparametric Statistical Methods*, Kendall's Library of Statistics, John Wiley and Sons, New York, 1998.

[12] D. Jungnickel, *Finite Fields, Structure and Arithmetics*, Bibliographisches Institut, Mannheim, 1993.

[13] E. L. Lehmann, *Nonparametrics: Statistical Methods Based on Ranks*, Springer, New York, 2006.

[14] R. Lidl and H. Niederreiter, *Introduction to Finite Fields and Their Applications*, Cambridge University Press, Cambridge, 1994.

[15] H. B. Mann and D. R. Whitney, *On a test of whether one of two random variables is stochastically larger than the other*, Ann. Math. Stat. **18**(1) (1947), 50–60.

[16] A. J. Menezes, I. F. Blake, S. Gao, R. C. Mullin, S. A. Vanstone, and T. Yaghoobian, *Applications of Finite Fields*, Kluwer Academic Publishers, 1993.

[17] G. L. Mullen and D. Panario, *Handbook of Finite Fields*, Discrete Mathematics and its Applications, CRC Press, A Chapman and Hall Book, 2013.

[18] R. C. Mullin, I. M. Onyszchuk, S. A. Vanstone, and R. M. Wilson, *Optimal normal bases in $GF(p^n)$*, Discrete Appl. Math. **22**(2) (1989), 149–161.

[19] G. Seroussi and A. Lempel, *Factorization of symmetric matrices and trace orthogonal bases in finite fields*, SIAM J. Comput. **9**(4) (1980), 758–767.

[20] S. S. Shapiro and M. B. Wilk, *An analysis of variance test for normality (complete samples)*, Biometrika **52**(3-4) (1965), 591–611.

[21] R. De Graeve, B. Parisse, and B. Ycart, *Computer Algebra System Giac/Xcas, Version 1.2.3*, Université Joseph Fourier, Grenoble, 2017.

[22] S. Vinatier, *Eléments Explicites en Théorie Algébrique des Nombres*, Habilitation à Diriger des Recherches, 2013.

[23] Z. X. Wan and K. Zhou, *On the complexity of the dual basis of a type I optimal normal basis*, Finite Fields Appl. **13**(2) (2007), 411–417.

[24] F. Wilcoxon, *Individual comparisons by ranking methods*, Biom. Bull. **1**(6) (1945), 80–83.

Université de Limoges, 123, avenue Albert Thomas, 87060 Limoges, France
E-mail address: `Stephane.Blondeau-Da-Silva@ac-limoges.fr`