

## Discrepancy and diaphony of digital $(0, 1)$ -sequences in prime base

by

HENRI FAURE (Marseille)

**1. Introduction.** This article is devoted to a precise study of the discrepancies  $D^*$ ,  $D$ ,  $T$  and of the diaphony  $F$  of a class of digital  $(0, 1)$ -sequences in prime bases, the so-called NUT digital  $(0, 1)$ -sequences, generated by nonsingular upper triangular matrices. Apart from Number Theory, the interest for such sequences comes from the intensive use in numerical integration of their multidimensional versions, the digital  $(0, s)$ -sequences, which are themselves special cases of the more general  $(t, s)$ -sequences introduced by Niederreiter [10].

The main results on the irregularities of distribution of  $(t, s)$ -sequences are obtained via the elementary interval property which is characteristic of  $(t, s)$ -sequences, not necessarily digital; but this property is too rough to allow comparisons and classification inside a given class, for instance the class of digital  $(0, 1)$ -sequences in a fixed base  $b$ . The problem of digging into the structure of such sequences is very challenging and until now only few results have been obtained: apart from papers on the two-dimensional Hammersley point sets dating from several years (Halton–Zaremba, White, DeClerck, Faure), the only contribution we know of is that of Grozdanov [6] for the diaphony and the  $L_2$ -discrepancy  $T$  of special NUT digital  $(0, 1)$ -sequences in base  $b$  (by means of estimations of trigonometric sums).

But recently, a new breakthrough was achieved by Larcher and Pillichshammer via the Walsh series analysis in base 2. Actually they obtain an exact formula for the remainder (the discrepancy function) of arbitrary digital  $(0, m, 2)$ -nets in base 2 (and also improved bounds for digital  $(0, m, 3)$ -nets in base 2) from which they deduce bounds for arbitrary digital  $(0, 1)$ -sequences in base 2 (and for digital  $(0, 2)$ -sequences in base 2); in the

---

2000 *Mathematics Subject Classification*: 11K06, 11K31, 11K38.

*Key words and phrases*: discrepancy, diaphony, generalized van der Corput sequences, digital  $(0, 1)$ -sequences.

references we have only quoted the papers which are directly related to our study: [8], [9] and [12].

Motivated by these advances and by the problem stated at the end of [8], we tackled the question with the method we introduced for the generalized van der Corput sequences ([3] and [2]), which, roughly speaking, correspond to digital  $(0, 1)$ -sequences generated by diagonal matrices. Finally, we have found exact formulas for the discrepancies  $D^*$ ,  $D$ ,  $T$  and for the diaphony  $F$  of arbitrary NUT digital  $(0, 1)$ -sequences in any prime base  $b$ , in the same form as in [3] and [2], thus strengthening the relationship between these two families of sequences (see Theorems 1–4). An interesting consequence is that introducing nonzero entries above the diagonal induces important changes for  $D^*$  and  $T$  but has no effect on  $D$  and  $F$ . Moreover, our formulas show the radical difference between entries on the diagonal and entries above: the diagonal entries determine the permutations connecting the NUT digital  $(0, 1)$ -sequences to the generalized van der Corput sequences, modulo a translation which is tied up to the entries above the diagonal.

With Theorems 2 and 4, the asymptotic studies in [3] and [2] apply directly and, after computer search, should give very low (extreme) discrepancy and diaphony sequences. As to Theorems 1 and 3, further investigations are necessary to attempt a classification of good sequences with regard to  $D^*$  and  $T$ . These developments, as well as applications to  $(0, m, 2)$ -nets, will be considered in a forthcoming study, since they would lengthen the present paper too much and since it is self-contained with exact calculations. Another direction for future research is the general case of  $(0, 1)$ -sequences and  $(0, m, 2)$ -nets in base  $b$  generated by arbitrary matrices for which Larcher and Pillichshammer have already important results in base 2.

Sections 2 and 3 introduce the necessary material for the statement of results (Section 4) and the proofs (Sections 5 and 6).

**2. Discrepancy and diaphony.** In this section we give the main definitions we shall use for the various discrepancies and the diaphony.

Let  $\alpha, \beta \in [0, 1]$ ; the *interval*  $[\alpha, \beta[$  is the usual semi-open interval if  $\alpha < \beta$ , the set  $[0, \beta] \cup [\alpha, 1]$  if  $\alpha > \beta$ , and the empty set if  $\alpha = \beta$ .

Let  $X = (x_n)_{n \geq 1}$  be an infinite sequence in  $[0, 1]$ ,  $N \geq 1$  an integer and  $[\alpha, \beta[$  an interval in  $[0, 1]$ ; the *remainder* (or *error*) to ideal distribution is the difference

$$E([\alpha, \beta]; N; X) = A([\alpha, \beta]; N; X) - Nl([\alpha, \beta]),$$

where  $A([\alpha, \beta]; N; X)$  is the number of indices  $n$  such that  $1 \leq n \leq N$  and  $x_n \in [\alpha, \beta[$ , and  $l([\alpha, \beta])$  is the length of  $[\alpha, \beta[$ . Similarly, for a finite set  $S$  of integers, we define the remainder with indices  $n \in S$  by

$$E([\alpha, \beta]; S; X) = A([\alpha, \beta]; S; X) - \text{card}(S)l([\alpha, \beta]).$$

Moreover, to simplify the writing, we set

$$A(\beta, N, X) := A([0, \beta[; N; X), \quad E(\beta, N, X) := E([0, \beta[; N; X),$$

so that we have

$$E([\alpha, \beta[; N; X) = -E([\beta, \alpha[; N; X) = E(\beta, N, X) - E(\alpha, N, X),$$

and the same with  $S$ .

We now define the *extreme discrepancies*:

$$\begin{aligned} D(N, X) &= \sup_{0 \leq \alpha < \beta \leq 1} |E([\alpha, \beta[; N; X)|, \\ D^*(N, X) &= \sup_{0 \leq \alpha \leq 1} |E(\alpha, N, X)|, \\ D^+(N, X) &= \sup_{0 \leq \alpha \leq 1} E(\alpha, N, X), \\ D^-(N, X) &= \sup_{0 \leq \alpha \leq 1} (-E(\alpha, N, X)). \end{aligned}$$

Usually,  $D$  is called the extreme discrepancy and  $D^*$  the star discrepancy;  $D^+$  and  $D^-$  have no name and are linked to the preceding one's by

$$\begin{aligned} D(N, X) &= D^+(N, X) + D^-(N, X), \\ D^*(N, X) &= \max(D^+(N, X), D^-(N, X)). \end{aligned}$$

The  $L_2$ -discrepancy and the *diaphony* are defined by:

$$\begin{aligned} T(N, X) &= \left( \int_0^1 (E(\alpha, N, X))^2 d\alpha \right)^{1/2}, \\ F(N, X) &= \left( 2 \sum_{m=1}^{\infty} \frac{1}{m^2} \left| \sum_{n=1}^N \exp(2i\pi m x_n) \right|^2 \right)^{1/2}. \end{aligned}$$

The diaphony and the  $L_2$ -discrepancy are related by the formula of Koksma

$$T^2(N, X) = \left( \sum_{n=1}^N \left( \frac{1}{2} - x_n \right) \right)^2 + \frac{1}{4\pi^2} F^2(N, X).$$

Note that

$$\sum_{n=1}^N \left( \frac{1}{2} - x_n \right) = \int_0^1 E(\alpha, N, X) d\alpha;$$

therefore, another definition for the diaphony could be

$$F^2(N, X) = 2\pi^2 \int_0^1 \int_0^1 E^2([\alpha, \beta[; N; X) d\alpha d\beta.$$

This point of view shows the parallel shape of  $D$  and  $F$  with regard to  $D^*$  and  $T$  and will enlighten the parallel between the extreme discrepancy and the diaphony of NUT digital  $(0, 1)$ -sequences (Theorems 2 and 4 below).

**3. Van der Corput and digital (0, 1)-sequences and related functions.** First, we recall the definition of the generalized van der Corput sequences introduced in [3] and further investigated in [2] and [5]. Next, we do the same for the digital (0, 1)-sequences in base  $b$ , the one-dimensional case of digital (0,  $s$ )-sequences introduced in [4] which have been widely studied and generalized, especially by Niederreiter (among many publications, see for instance [10] and [11]). Finally, we recall the definition of the family of the so-called functions  $\varphi$ , functions associated with the generalized van der Corput sequences ([2] and [3]), which take also a leading part in the study of digital (0, 1)-sequences.

Our notation is in agreement with our preceding papers; in particular we index sequences with the integers  $N \geq 1$  and expand  $N - 1$  in the  $b$ -adic numeration system (this choice appears in the book of Kuipers and Niederreiter [7] and is also kept in [10]).

The generalized van der Corput sequences may be defined in fixed or variable bases; for simplicity, we restrict ourselves to fixed bases  $b$ , with  $b$  an integer  $\geq 2$ , not necessarily prime.

For integers  $n$  and  $N$  with  $n \geq 1$  and  $1 \leq N \leq b^n$ , write  $N - 1 = \sum_{r=0}^{\infty} a_r(N)b^r$  in the  $b$ -adic system (so that  $a_r(N) = 0$  if  $r \geq n$ ) and let  $\Sigma = (\sigma_r)_{r \geq 0}$  be a sequence of permutations of  $\{0, 1, \dots, b - 1\}$ . Then the *generalized van der Corput sequence*  $S_b^\Sigma$  in base  $b$  associated with  $\Sigma$  is defined by

$$S_b^\Sigma(N) = \sum_{r=0}^{\infty} \frac{\sigma_r(a_r(N))}{b^{r+1}}.$$

The definition of digital (0, 1)-sequences in base  $b$  results from the general construction principle of Niederreiter [10], but in this paper we shall be concerned with a special case which can be simply described as follows. We consider only *prime* bases  $b$  and the finite field  $\mathbb{F}_b$  is identified as a set with  $\{0, 1, \dots, b - 1\}$ . In all computations involving elements of  $\mathbb{F}_b$ , addition and multiplication are performed in  $\mathbb{F}_b$ ; we do not choose special symbols for them, but sometimes we add “(mod  $b$ )” to avoid confusion.

The *digital (0, 1)-sequences in base  $b$*  we study are defined by

$$X_b^C = (x_N)_{N \geq 1} \quad \text{with} \quad x_N = \sum_{r=0}^{\infty} \frac{x_{N,r}}{b^{r+1}}, \quad x_{N,r} = \sum_{k=r}^{\infty} c_r^k a_k(N) \pmod{b},$$

the generator matrix  $C = (c_r^k)_{r \geq 0, k \geq 0}$  being an infinite *nonsingular upper triangular* (NUT) matrix with entries  $c_r^k \in \mathbb{F}_b$  (by the definitions of  $a_k(N)$  and  $C$ , the summations above are finite). In brief, we name these sequences *NUT digital (0, 1)-sequences*.

Note that this class of sequences contains all one-dimensional projections of digital  $(0, s)$ -sequences whose generator matrices are NUT, in particular those obtained by multiplying on the left the classical powers of Pascal matrices by diagonal matrices.

For future use in Lemma 6.2, we recall the important *elementary interval property* satisfied by the  $(0, 1)$ -sequences in base  $b$  in general.

An *elementary interval in base  $b$*  is an interval of the form

$$E = [ab^{-d}, (a + 1)b^{-d}[$$

with  $a, d$  integers such that  $d \geq 0$  and  $0 \leq a < b^d$ . Then

for all integers  $l, m \geq 0$ , every elementary interval  $E$  with  $l(E) = b^{-m}$  contains exactly one point of the section  $(x_{lb^{m+1}}, \dots, x_{(l+1)b^m})$  of the sequence.

Functions  $\varphi_{b,h}^\sigma$  related to a pair  $(b, \sigma)$ , with  $\sigma$  a permutation of  $\mathbb{F}_b$ . Set

$$Z_b^\sigma = \left( \frac{\sigma(0)}{b}, \dots, \frac{\sigma(b-1)}{b} \right).$$

For any integer  $h$ ,  $0 \leq h \leq b-1$ , the function  $\varphi_{b,h}^\sigma$  (from  $\mathbb{R}$  to  $\mathbb{R}$ ) is defined as follows. Let  $k$  be an integer with  $1 \leq k \leq b$ . Then for  $x \in [(k-1)/b, k/b[$  we set

$$\varphi_{b,h}^\sigma(x) = \begin{cases} A(h/b, k, Z_b^\sigma) - hx & \text{if } 0 \leq h \leq \sigma(k-1), \\ (b-h)x - A([h/b, 1[; k; Z_b^\sigma) & \text{if } \sigma(k-1) < h < b; \end{cases}$$

then the function  $\varphi_{b,h}^\sigma$  is extended to the reals by periodicity. Note that  $\varphi_{b,0}^\sigma = 0$ .

Thus we have associated  $b$  functions with the pair  $(b, \sigma)$ :

$$\varphi_{b,0}^\sigma = 0, \varphi_{b,1}^\sigma, \dots, \varphi_{b,b-1}^\sigma.$$

In the very special case  $b = 2$ , we only have two permutations which give either  $\varphi_{2,1}^\sigma = \|\cdot\|$ , if  $\sigma$  is the identical permutation, or  $\varphi_{2,1}^\sigma = -\|\cdot\|$ , if  $\sigma = (0 \ 1)$ , where  $\|\cdot\|$  is the distance to the nearest integer. So, we are not astonished by the title of the important paper [9], since it deals with digital  $(0, m, 2)$ -nets in base 2, which are nets with close relations to digital  $(0, 1)$ -sequences in base 2, to begin with the original van der Corput sequence (see [1] for a precise study). Of course, as  $b$  grows up, the functions  $\varphi_{b,h}^\sigma$  become more and more numerous and complicated, but they are the necessary keys to express the error  $E(\alpha, N, X)$  and to obtain exact formulas for the discrepancies and the diaphony of the sequences  $S_b^\Sigma$  and  $X_b^C$ . Actually, the functions  $\varphi_{b,h}^\sigma$  give rise to other functions, depending only on  $(b, \sigma)$ , according to the applied notion of discrepancy, as we shall see in the next section. For the present, we recall the main properties we shall use.

PROPERTY 3.0. *The functions  $\varphi_{b,h}^\sigma$  are continuous and piecewise affine; the absolute values of the coefficients involved in the affine functions are less than  $b - 1$ ; moreover*

$$|\varphi_{b,h}^\sigma| \leq b/4, \quad (\varphi_{b,h}^\sigma)'(k/b) = (\varphi_{b,h}^I)'(\sigma(k)/b),$$

where  $k$  is an integer with  $0 \leq k \leq b - 1$  and where  $f'$  denotes the right derivative of  $f$  and  $I$  the identical permutation.

The proof is scattered in [2, Properties 3.3 and 3.4], and in [3, Properties 3.2.1 and 3.2.2] (the proofs of the last two properties apply to the  $(\varphi_{b,h}^\sigma)$ 's even though they are given in [3] for the  $(\psi_b^\sigma)$ 's introduced below).

**4. Statement of the results.** We begin by recalling some results on generalized van der Corput sequences, through which we introduce new functions and which illustrate the links and differences between the two families of sequences.

**4.1. Results for generalized van der Corput sequences.** These results come from [2] and [3]. We are only concerned here with exact formulas; we refer to the papers above for various asymptotic relations resulting from these formulas.

*Formulas for the extreme discrepancies.* Set

$$\psi_b^{\sigma,+} = \max_{0 \leq h \leq b-1} (\varphi_{b,h}^\sigma), \quad \psi_b^{\sigma,-} = \max_{0 \leq h \leq b-1} (-\varphi_{b,h}^\sigma), \quad \psi_b^\sigma = \psi_b^{\sigma,+} + \psi_b^{\sigma,-}.$$

Then, for all  $N \geq 1$ , we have

$$\begin{aligned} D^+(N, S_b^\Sigma) &= \sum_{j=1}^{\infty} \psi_b^{\sigma_{j-1},+} \left( \frac{N}{b^j} \right), \\ D^-(N, S_b^\Sigma) &= \sum_{j=1}^{\infty} \psi_b^{\sigma_{j-1},-} \left( \frac{N}{b^j} \right), \\ D(N, S_b^\Sigma) &= \sum_{j=1}^{\infty} \psi_b^{\sigma_{j-1}} \left( \frac{N}{b^j} \right), \\ D^*(N, S_b^\Sigma) &= \max(D^+(N, S_b^\Sigma), D^-(N, S_b^\Sigma)). \end{aligned}$$

*Formulas for  $L_2$ -discrepancy and diaphony.* Set

$$\varphi_b^\sigma = \sum_{h=0}^{b-1} \varphi_{b,h}^\sigma, \quad \phi_b^\sigma = \sum_{h=0}^{b-1} (\varphi_{b,h}^\sigma)^2, \quad \chi_b^\sigma = b\phi_b^\sigma - (\varphi_b^\sigma)^2.$$

Then, for all  $N \geq 1$ , we have

$$T^2(N, S_b^\Sigma) = \frac{1}{b} \sum_{j=1}^{\infty} \phi_b^{\sigma_{j-1}} \left( \frac{N}{bj} \right) + \frac{1}{b^2} \sum_{i \neq j} \varphi_b^{\sigma_{i-1}} \left( \frac{N}{b^i} \right) \varphi_b^{\sigma_{j-1}} \left( \frac{N}{bj} \right),$$

$$\frac{1}{4\pi^2} F^2(N, S_b^\Sigma) = \frac{1}{b^2} \sum_{j=1}^{\infty} \chi_b^{\sigma_{j-1}} \left( \frac{N}{bj} \right).$$

Note that

$$\psi_b^\sigma = \max_{0 \leq h < h' \leq b-1} |\varphi_{b,h}^\sigma - \varphi_{b,h'}^\sigma|, \quad \chi_b^\sigma = \sum_{0 \leq h < h' \leq b-1} (\varphi_{b,h}^\sigma - \varphi_{b,h'}^\sigma)^2;$$

these properties will be useful for the proofs of Theorems 2 and 4.

**4.2. Results for NUT digital  $(0, 1)$ -sequences in prime base.** We recall that we deal only with sequences  $X_b^C$  generated by NUT matrices  $C$ . Before stating our theorems, we need more notations to take into account the complexity introduced by the entries above the diagonal. Indeed, if the generator matrix  $C$  is diagonal, we have  $X_b^C = S_b^\Delta$  with  $\Delta = (\delta_r)_{r \geq 0}$  the sequence of permutations of  $\mathbb{F}_b$  defined by  $\delta_r(i) = c_r^* i$ , i.e.  $\delta_r$  is the multiplication in  $\mathbb{F}_b$  by the diagonal entry  $c_r^*$ . Now, if  $C$  is not diagonal, as we shall see in Property 5.3 and Lemma 6.2 in the next sections, the diagonal entries will still determine the same permutations  $\delta_r$ , but the permutations  $\sigma_r$  that will give the exact formulas for  $D^+$ ,  $D^-$ ,  $D^*$  and  $T$  will be translated permutations (depending on  $N \geq 1$ ) of the  $\delta_r$ 's, according to the following rule: for all  $r \geq 0$  and  $i \in \mathbb{F}_b$ ,

$$\sigma_r(i) = \delta_r(i) + \sum_{k=r+1}^{\infty} c_r^k a_k(N) \pmod{b}$$

where  $N - 1 = \sum_{r=0}^{\infty} a_r(N) b^r$  in the  $b$ -adic system.

For convenience of notation, we shall use the symbol  $\uplus$  for such translations: for  $\delta$  a permutation of  $\mathbb{F}_b$  and  $t \in \mathbb{F}_b$ , we write  $\delta \uplus t$  to mean the permutation defined by  $(\delta \uplus t)(i) := \delta(i) + t$  for all  $i \in \mathbb{F}_b$ , so that the permutation above is

$$\sigma_r = \delta_r \uplus \theta_r(N) \quad \text{with} \quad \theta_r(N) = \sum_{k=r+1}^{\infty} c_r^k a_k(N).$$

Note that  $a_k(N) = 0$  for all  $k \geq n$  if  $1 \leq N \leq b^n$ , thus  $\theta_r(N) = 0$  and  $\sigma_r = \delta_r$  for all  $r \geq n - 1$  in this case.

With the definitions of the functions  $\psi_b^{\sigma,+}$ ,  $\psi_b^{\sigma,-}$ ,  $\psi_b^\sigma$ ,  $\varphi_b^\sigma$ ,  $\phi_b^\sigma$  and  $\chi_b^\sigma$  (see 4.1) and with the definitions of  $\delta_r$ ,  $\theta_r(N)$  and  $\delta_r \uplus \theta_r(N)$  given above, we are in a position to state our theorems.

THEOREM 1. For all NUT matrices  $C$  and all integers  $N \geq 1$ ,

$$D^+(N, X_b^C) = \sum_{j=1}^{\infty} \psi_b^{\delta_{j-1} \uplus \theta_{j-1}(N), +} \left( \frac{N}{b^j} \right),$$

$$D^-(N, X_b^C) = \sum_{j=1}^{\infty} \psi_b^{\delta_{j-1} \uplus \theta_{j-1}(N), -} \left( \frac{N}{b^j} \right),$$

$$D^*(N, X_b^C) = \max(D^+(N, X_b^C), D^-(N, X_b^C)).$$

THEOREM 2. For all NUT matrices  $C$  and all integers  $N \geq 1$ ,

$$D(N, X_b^C) = \sum_{j=1}^{\infty} \psi_b^{\delta_{j-1}} \left( \frac{N}{b^j} \right).$$

THEOREM 3. For all NUT matrices  $C$  and all integers  $N \geq 1$ ,

$$T^2(N, X_b^C) = \frac{1}{b} \sum_{j=1}^{\infty} \phi_b^{\delta_{j-1} \uplus \theta_{j-1}(N)} \left( \frac{N}{b^j} \right) + \frac{1}{b^2} \sum_{i \neq j} \varphi_b^{\delta_{i-1} \uplus \theta_{i-1}(N)} \left( \frac{N}{b^i} \right) \varphi_b^{\delta_{j-1} \uplus \theta_{j-1}(N)} \left( \frac{N}{b^j} \right).$$

THEOREM 4. For all NUT matrices  $C$  and all integers  $N \geq 1$ ,

$$\frac{1}{4\pi^2} F^2(N, X_b^C) = \frac{1}{b^2} \sum_{j=1}^{\infty} \chi_b^{\delta_{j-1}} \left( \frac{N}{b^j} \right).$$

REMARKS. 1. The formulas of Theorems 1 and 3 for  $D^+$ ,  $D^-$ ,  $D^*$  and  $T$  involve the quantity  $\theta_{j-1}(N)$  which depends on  $N$  via the  $b$ -adic expansion of  $N - 1$  and on the generator NUT matrix  $C$  via its entries above the diagonal; this dependence is a big handicap for the precise study of the asymptotic behaviour which should be quite different according to these entries. In relation with this awkward problem, we refer to the paper of Pillichshammer [12] who, in base 2, obtains the foremost result in this direction for  $D^*$ .

2. On the contrary, the formulas of Theorems 2 and 4 for  $D$  and  $F$  depend only on the permutations  $\delta_r$ , that is, on the diagonal entries of  $C$ . This remarkable feature shows that digital  $(0, 1)$ -sequences generated by NUT matrices having the same diagonal have the same extreme discrepancy and the same diaphony. In this case, the study of the asymptotic behaviour for the generalized van der Corput sequences ([2] and [3]) applies with the specific permutations  $\delta$  obtained by multiplication in the finite field  $\mathbb{F}_b$ .

3. Until now, only results in base 2 have been available from the studies of digital  $(0, m, 2)$ -nets in base 2 by Larcher and Pillichshammer ([8], [9] and [12]), except for the diaphony and the  $L_2$ -discrepancy for which Groz-

danov [6] obtained upper bounds in base  $b$  in the special case of NUT matrices  $C$  with  $c_r^r = 1$ .

COROLLARY. *For all integers  $n$  and  $N$  with  $1 \leq N \leq b^n$ ,*

$$D^+(N, X_b^C) = \sum_{j=1}^n \psi_b^{\delta_{j-1} \uplus \theta_{j-1}(N), +} \left( \frac{N}{b^j} \right) + \frac{N}{b^n},$$

$$D^-(N, X_b^C) = \sum_{j=1}^n \psi_b^{\delta_{j-1} \uplus \theta_{j-1}(N), -} \left( \frac{N}{b^j} \right),$$

$$D(N, X_b^C) = \sum_{j=1}^n \psi_b^{\delta_{j-1}} \left( \frac{N}{b^j} \right) + \frac{N}{b^n},$$

$$\frac{1}{4\pi^2} F^2(N, X_b^C) = \frac{1}{b^2} \sum_{j=1}^n \chi_b^{\delta_{j-1}} \left( \frac{N}{b^j} \right) + \frac{N^2}{12b^{2n}},$$

$$T^2(N, X_b^C) = \left( \frac{1}{b} \sum_{j=1}^n \varphi_b^{\delta_{j-1} \uplus \theta_{j-1}(N)} \left( \frac{N}{b^j} \right) + \frac{N}{2b^n} \right)^2 + \frac{1}{b^2} \sum_{j=1}^n \chi_b^{\delta_{j-1}} \left( \frac{N}{b^j} \right) + \frac{N^2}{12b^{2n}}.$$

This Corollary is a useful tool for computations; it is also the starting point for the research of bounds and for the study of the asymptotic behaviour of the discrepancies and the diaphony. See Remark 2 above for  $D$  and  $F$ ; as to  $D^+$ ,  $D^-$  and  $T$ , apart from trivial bounds, further investigations are necessary to obtain sharp results depending on the entries above the diagonals of the generator matrices.

**5. First properties of NUT digital  $(0, 1)$ -sequences.** This section is devoted to three properties, resulting from the matrix construction of the sequences, which are necessary to prove the fundamental Lemma 6.2.

We introduce more notations we shall use in Sections 5 and 6 to simplify the writing: let  $X := X_b^C$ ,  $Y := S_b^I$  ( $I$  is the identical permutation),  $X_n := (x_1, \dots, x_{b^n})$ ,  $Y_n := (y_1, \dots, y_{b^n})$  and denote by  $\bar{X}_n$  (resp.  $\bar{Y}_n$ ) the support of  $X_n$  (resp.  $Y_n$ ). Actually,  $\bar{X}_n = \bar{Y}_n$  since  $x_1 = y_1$ , but we keep the two notations to avoid confusion in the proofs. Moreover, we define the sections  $X_m^l := (x_{lb^m+1}, \dots, x_{(l+1)b^m})$  of  $X$  for all nonnegative integers  $l, m$  (so  $X_n = X_n^0$ ).

**5.1. PROPERTY.** *Let  $n \geq 1$ ; the terms of  $X_n$  are the vertices (including 0) of the regular polygon of  $b^n$  edges inscribed in  $[0, 1]$  identified to the unit torus.*

Moreover, let  $i, j$  be integers, with  $1 \leq i \leq b^{n-1}$  and  $0 \leq j < b$ , and suppose  $x_i = x_{i, n-2} b^{-n+1} + \dots + x_{i,0} b^{-1}$  is the  $b$ -adic expansion of  $x_i$ . Then

$$x_{i+jb^{n-1}} = c_{n-1}^{n-1} j b^{-n} + (x_{i, n-2} + c_{n-2}^{n-1} j) b^{-n+1} + \dots + (x_{i,0} + c_0^{n-1} j) b^{-1}$$

is the  $b$ -adic expansion of  $x_{i+jb^{n-1}}$  (in which of course the digits  $c_{n-1}^{n-1} j$  and  $x_{i, n-k} + c_{n-k}^{n-1} j$  are computed mod  $b$ ).

*Proof.* The NUT matrix  $C$  induces a bijection from the set of integers between 1 and  $b^n$  onto  $\bar{X}_n$  which identifies the terms of  $X_n$  with the vertices of the polygon; hence the first part.

The second part is also straightforward since

$$\begin{pmatrix} c_0^0 & \dots & c_0^{n-2} & c_0^{n-1} \\ \vdots & \ddots & \vdots & \vdots \\ 0 & \dots & c_{n-2}^{n-2} & c_{n-2}^{n-1} \\ 0 & \dots & 0 & c_{n-1}^{n-1} \end{pmatrix} \begin{pmatrix} a_0(i) \\ \vdots \\ a_{n-2}(i) \\ j \end{pmatrix} = \begin{pmatrix} \sum_{k=0}^{n-2} c_0^k a_k(i) + c_0^{n-1} j \\ \vdots \\ c_{n-2}^{n-2} a_{n-2}(i) + c_{n-2}^{n-1} j \\ c_{n-1}^{n-1} j \end{pmatrix}$$

and  $\sum_{k=0}^{n-2} c_0^k a_k(i) = x_{i,0}, \dots, c_{n-2}^{n-2} a_{n-2}(i) = x_{i, n-2}$  by definition of  $X_b^C$ . ■

**5.2. PROPERTY.** Let  $n \geq 1$ ,  $u \in \bar{Y}_{n-1}$  with  $b$ -adic expansion  $u = \sum_{r=0}^{n-2} u_r b^{-r-1}$  and  $v = u + b^{-n+1}$ . Then the interval  $[u, v[$  contains exactly  $b$  terms of  $X_n$  which are given in increasing order by

$$u = x_{i_0+j_0 b^{n-1}} < x_{i_1+j_1 b^{n-1}} < \dots < x_{i_{b-1}+j_{b-1} b^{n-1}} < v,$$

where, for  $0 \leq \mu \leq b-1$ ,  $j_\mu = \mu / c_{n-1}^{n-1} = \delta_{n-1}^{-1}(\mu)$  and  $i_\mu$ , with  $1 \leq i_\mu \leq b^{n-1}$ , is a well defined integer depending on  $u$  (its determination will result from the proof). Therefore, the order of the terms of  $X_n$  in  $[u, v[$  is independent of  $u \in \bar{Y}_{n-1}$  and is the same as the order of the terms of  $Z_b^{\delta_{n-1}}$  in  $[0, 1[$  given by

$$0 = \delta_{n-1}(j_0) < \delta_{n-1}(j_1) < \dots < \delta_{n-1}(j_{b-1}) = b - 1.$$

*Proof.* By Property 5.1, we already know that there are  $b$  terms of  $X_n$  in  $[u, v[$  since  $\bar{X}_n$  and  $\bar{X}_{n-1}$  are regular polygons having the vertex 0. But in contrast to the study of the generalized van der Corput sequences  $S_b^\Sigma$  ([3, Prop. 3.1.3], [2, Prop. 3.2]), the terms of  $X_n$  in  $[u, v[$  are not determined by the indices  $i + j b^{n-1}$  of Property 5.1 for fixed  $i$  and  $0 \leq j < b$ ; the situation is now more complicated and the index  $i$  is not fixed; moreover, the entries of  $C$  above the diagonal introduce perturbations which require a specific treatment for the sections of  $X_n$ ; that will be the purpose of the next Property 5.3.

To prove the present one, we consider the system (\*) below in the unknowns  $z_r$  with a given  $0 \leq \mu \leq b-1$ ; clearly the solution will give the digits of the  $b$ -adic expansion of  $l-1$ , with  $l$  the index of  $x_l = u + \mu b^{-n}$ , the  $\mu$ th term (in increasing order) of  $X_n$  in  $[u, v[$ :

$$(*) \quad \begin{pmatrix} c_0^0 & \cdots & c_0^{n-2} & c_0^{n-1} \\ \vdots & \ddots & \vdots & \vdots \\ 0 & \cdots & c_{n-2}^{n-2} & c_{n-2}^{n-1} \\ 0 & \cdots & 0 & c_{n-1}^{n-1} \end{pmatrix} \begin{pmatrix} z_0 \\ \vdots \\ z_{n-2} \\ z_{n-1} \end{pmatrix} = \begin{pmatrix} u_0 \\ \vdots \\ u_{n-2} \\ \mu \end{pmatrix}.$$

Thus, we find  $z_{n-1} = \mu/c_{n-1}^{n-1} = \delta_{n-1}^{-1}(\mu) = j_\mu$  and the index  $i_\mu$  in  $x_l = x_{i_\mu+j_\mu b^{n-1}} = u + \mu b^{-n}$  is defined by  $i_\mu - 1 = z_0 + \cdots + z_{n-2}b^{n-2}$ , where  $(z_0, \dots, z_{n-2})$  is the solution of (\*) with  $z_{n-1} = j_\mu$ . Therefore (note that  $j_0 = 0$ ),

$$u = x_{i_0} < x_{i_1+j_1 b^{n-1}} < \cdots < x_{i_{b-1}+j_{b-1} b^{n-1}} < v.$$

On the other hand, since  $\delta_{n-1}(j_\mu) = \mu$ , we also have

$$0 = \frac{\delta_{n-1}(j_0)}{b} < \frac{\delta_{n-1}(j_1)}{b} < \cdots < \frac{\delta_{n-1}(j_{b-1})}{b} = \frac{b-1}{b},$$

which is the order of the terms of  $Z_b^{\delta_{n-1}}$  in  $[0, 1[$  in increasing order, thus the last part of Property 5.2. ■

**5.3. PROPERTY.** *Let  $n$  and  $s$  be integers with  $2 \leq s \leq n$ ; let  $u \in \bar{Y}_{n-s}$ , with  $b$ -adic expansion  $u = \sum_{r=0}^{n-s-1} u_r b^{-r-1}$  ( $u = 0$  if  $s = n$ ), and  $v = u + b^{-n+s}$ ; let  $A_{n-s+1} := \sum_{r=n-s+1}^{n-1} z_r b^r$  with arbitrary given digits  $z_{n-1}, \dots, z_{n-s+1}$  and let  $S_{n-s+1} := X_{n-s+1}^{A_{n-s+1} b^{-n+s-1}}$  be the corresponding section of  $X_n$ . Then the interval  $[u, v[$  contains exactly  $b$  terms of  $S_{n-s+1}$  which are given in increasing order by*

$$u = x_{i_0+j_0 b^{n-s}+A_{n-s+1}} < x_{i_1+j_1 b^{n-s}+A_{n-s+1}} < \cdots < x_{i_{b-1}+j_{b-1} b^{n-s}+A_{n-s+1}} < v,$$

where, for  $0 \leq \mu \leq b-1$ ,  $j_\mu = \sigma_{n-s}^{-1}(\mu)$  and  $i_\mu$  ( $1 \leq i_\mu \leq b^{n-s}$ ) is an integer depending on  $u$ . Therefore, the order of the terms of  $S_{n-s+1}$  in  $[u, v[$  is independent of  $u \in \bar{Y}_{n-s}$  and is the same as the order of the terms of  $Z_b^{\sigma_{n-s}}$  in  $[0, 1[$  given by

$$0 = \sigma_{n-s}(j_0) < \sigma_{n-s}(j_1) < \cdots < \sigma_{n-s}(j_{b-1}) = b-1.$$

*Proof.* We consider the following system in the unknowns  $z_0, \dots, z_{n-s}$  with parameters  $z_{n-s+1}, \dots, z_{n-1}$  and  $\mu$  ( $0 \leq \mu \leq b-1$ ):

$$(**) \quad \begin{pmatrix} c_0^0 & \cdots & c_0^{n-s-1} & c_0^{n-s} & \cdots & c_0^{n-1} \\ \vdots & \ddots & \vdots & \vdots & \vdots & \vdots \\ 0 & \cdots & c_{n-s-1}^{n-s-1} & c_{n-s-1}^{n-s} & \cdots & c_{n-s-1}^{n-1} \\ 0 & \cdots & 0 & c_{n-s}^{n-s} & \cdots & c_{n-s}^{n-1} \end{pmatrix} \begin{pmatrix} z_0 \\ \vdots \\ z_{n-s} \\ z_{n-s+1} \\ \vdots \\ z_{n-1} \end{pmatrix} = \begin{pmatrix} u_0 \\ \vdots \\ u_{n-s-1} \\ \mu \end{pmatrix}.$$

As in Property 5.2, the solution will give the digits of the  $b$ -adic expansion of  $l - 1$  with  $l$  the index of  $x_l = u + \mu b^{-n+s-1}$ , the  $\mu$ th term of the section  $S_{n-s+1}$  of  $X_n$  in  $[u, v]$ .

First, we obtain  $\mu = c_{n-s}^{n-s} z_{n-s} + \cdots + c_{n-s}^{n-1} z_{n-1}$ , that is,

$$z_{n-s} = \frac{\mu - c_{n-s}^{n-s+1} z_{n-s+1} + \cdots + c_{n-s}^{n-1} z_{n-1}}{c_{n-s}^{n-s}} = j_\mu = \sigma_{n-s}^{-1}(\mu),$$

where  $\sigma_{n-s} = \delta_{n-s} \uplus \theta_{n-s}$  with  $\theta_{n-s} = \sum_{i=1}^{s-1} c_{n-s}^{n-i} z_{n-i}$  (here appears the rule we introduced in principle in 4.2).

Next, the integer  $i_\mu$  in  $x_l = x_{i_\mu + j_\mu b^{n-s}} = u + \mu b^{-n+s-1}$  is defined by  $i_\mu - 1 = z_0 + \cdots + z_{n-s-1} b^{n-s-1}$  where  $z_0, \dots, z_{n-s-1}$  are the other solutions of (\*\*). Note that  $i_\mu = 1$  if  $s = n$  since (\*\*) reduces to one equation in the unknown  $z_0$  in this case.

The end of the proof is similar to the preceding one. ■

## 6. Proofs of the theorems and the Corollary

**6.1. LEMMA** (discretization). *Let  $n$  and  $N$  be two integers with  $1 \leq N \leq b^n$  and let  $\alpha \in [0, 1]$ . Then*

$$E(\alpha, N, X_b^C) = E(y(\alpha), N, X_b^C) + (y(\alpha) - \alpha)N$$

with  $y(\alpha) = u$  if  $\alpha = u$  and  $y(\alpha) = v$  if  $\alpha > u$ , where  $u$  and  $v$  are the unique elements of  $[0, 1]$  such that  $u \in \bar{Y}_n$ ,  $v = u + b^{-n}$  and  $u \leq \alpha < v$ .

*Proof.* By definition of  $y(\alpha)$ , we have  $A(\alpha, N, X_b^C) = A(y(\alpha), N, X_b^C)$ , from which the result follows, since  $u$  is the unique term of  $X_n$  in  $[u, v]$ . ■

**6.2. LEMMA** (descent). *Let  $n, N$  and  $\lambda$  be integers with  $1 \leq N \leq b^n$  and  $1 \leq \lambda < b^n$  and let  $\lambda = \lambda_1 b^{n-1} + \cdots + \lambda_{n-1} b + \lambda_n$  be the  $b$ -adic expansion of  $\lambda$ . Then*

$$E\left(\frac{\lambda}{b^n}, N, X_b^C\right) = \sum_{j=1}^n \varphi_{b, \varepsilon_j}^{\delta_{j-1} \uplus \theta_{j-1}(N)} \left(\frac{N}{bj}\right),$$

the  $\varepsilon_j$ 's being defined step by step as follows:  $\varepsilon_n = \eta_n = \lambda_n$  and,

for  $1 \leq j < n$ ,

$$\eta_j = \lambda_j + \frac{\eta_{j+1}}{b} + \frac{1}{b} (\varphi_{b, \varepsilon_{j+1}}^{\delta_j \uplus \theta_j(N)})' \left( \frac{N}{b^{j+1}} \right),$$

$$\varepsilon_j = \eta_j \quad \text{if } 0 \leq \eta_j < b, \quad \varepsilon_j = 0 \quad \text{if } \eta_j = b.$$

REMARKS. Of course, the  $\varepsilon_j$ 's depend on  $\lambda$ ,  $n$  and  $N$ . See 4.2 for the definition of  $\delta_{j-1} \uplus \theta_{j-1}(N)$ . Note also that for  $\lambda = b^n$  the formula is trivially true with  $\varepsilon_j = 0$  for all  $1 \leq j \leq n$ .

*Foreword.* This lemma is the key lemma for the proofs of our theorems; step by step, we obtain the remainder  $E$  by means of remainders with more and more rough intervals and with fewer and fewer points; at each step, the difference between the remainders is under control with the help of the functions  $\varphi_{b,h}^\sigma$  while the relation between the intervals depends on the right derivatives of these functions.

*Notations.* To simplify the writing, we shall use the  $b$ -adic expansion of  $N < b^n$ . Let  $r_0$  be the greatest nonnegative integer such that  $b^{r_0}$  divides  $N$ ; then we write  $N = N_{n-1}b^{n-1} + \dots + N_{r_0}b^{r_0}$  with  $N_{r_0} \neq 0$ ; the digits  $N_r$  are related to those of the  $b$ -adic expansion of  $N - 1$  by  $N_r = a_r(N)$  if  $r_0 < r \leq n - 1$  and  $N_{r_0} = a_{r_0}(N) + 1$ .

Moreover, with the same concern, we introduce one more piece of notation: for  $r_0 \leq j \leq n - 1$  we define the slice of integers

$$T_j := ]N_{n-1}b^{n-1} + \dots + N_jb^j, N] \quad (\text{note that } T_{r_0} \text{ is empty})$$

and we recall that we have already set  $S_j := X_j^{A_j b^{-j}}$  (see Property 5.3 with here  $j = n - s + 1$  and  $N_r = z_r$ ).

*Proof of Lemma 6.2.* The case  $N = b^n$  is trivial since both terms of the equality to be proved are zero because  $A(\lambda/b^n, b^n, X_n) = \lambda$  and the functions  $\varphi$  are zero on the integers. From now on we suppose  $N < b^n$ .

FIRST STEP. Set  $y = \lambda/b^n \in \bar{Y}_n$ ; there exist unique  $u, v$  such that  $u \in \bar{Y}_{n-1}$ ,  $v = u + 1/b^{n-1}$  and  $u \leq y < v$ . According to Property 5.2, there exists a unique index  $i$  such that  $1 \leq i \leq b^{n-1}$  and  $x_{i+N_{n-1}b^{n-1}} \in \bar{X}_n \cap [u, v[$ ; to get it we should solve the system (\*) with  $\mu = \delta_{n-1}(N_{n-1})$ ; but we do not need that because to express the remainder  $E(y, N, X_n)$ , as shown below, we are only interested in the position of  $x_{i+N_{n-1}b^{n-1}}$  in  $[u, v[$  which is independent of  $u$ . We distinguish two cases:

CASE 1. If  $y \leq x_{i+N_{n-1}b^{n-1}}$  then with  $y^1 = u$  we have

$$E(y, N, X_n) = E(y^1, N, X_n) + A([y^1, y]; N; X_n) - N(y - y^1).$$

Now,  $A([y^1, y]; N; X_n) = A(\lambda_n/b, N_{n-1} + 1, Z_b^{\delta_{n-1}})$  because the order of the terms of  $X_n$  in  $[u, v[$  is the same as the order of the terms of  $Z_b^{\delta_{n-1}}$  in  $[0, 1[$

and, on the other hand,  $y - y^1 = \lambda_n/b^n$ . Moreover,  $N(y - y^1) = \varepsilon_n N/b^n$  (since  $\varepsilon_n = \lambda_n$ ) and  $0 \leq \lambda_n \leq \delta_{n-1}(N_{n-1})$  (since  $u \leq y \leq x_{i+N_{n-1}b^{n-1}} < v$  with  $v - u = 1/b^{n-1}$  and  $x_{i+N_{n-1}b^{n-1}, n-1} = \delta_{n-1}(N_{n-1})$ ); in other words,  $y$  and  $x_{i+N_{n-1}b^{n-1}}$  have the same digits except the last ones which are  $\lambda_n$  and  $c_{n-1}^{n-1}N_{n-1} = \delta_{n-1}(N_{n-1})$  from Property 5.1.

Therefore, according to the definition of the functions  $\varphi$ , we have

$$A([y^1, y[; N; X_n) - N(y - y^1) = \varphi_{b, \varepsilon_n}^{\delta_{n-1}}(N/b^n)$$

and so

$$E(y, N, X_n) = E(y^1, N, X_n) + \varphi_{b, \varepsilon_n}^{\delta_{n-1}}(N/b^n).$$

Note that if  $N_{n-1} = 0$  then  $y = y^1 = u$  (because  $u = y^1 \leq y \leq x_i = u$  since  $x_i \in \bar{X}_{n-1}$ ) and  $\varepsilon_n = \lambda_n = 0$ .

Finally,

$$\lambda^1 := y^1 b^{n-1} = (\lambda + (\varphi_{b, \varepsilon_n}^{\delta_{n-1}})'(N/b^n))/b$$

since here we have  $(\varphi_{b, \varepsilon_n}^{\delta_{n-1}})'(N/b^n) = -\varepsilon_n$ .

CASE 2. If  $y > x_{i+N_{n-1}b^{n-1}}$  then with  $y^1 = v$  and  $\varepsilon_n = \lambda_n$ , in the same way, we get

$$\begin{aligned} E(y, N, X_n) &= E(y^1, N, X_n) - A([y, y^1[; N; X_n) + N(y^1 - y) \\ &= E(y^1, N, X_n) + \varphi_{b, \varepsilon_n}^{\delta_{n-1}}(N/b^n) \end{aligned}$$

because  $A([y, y^1[; N; X_n) = A([\lambda_n/b, 1[; N_{n-1} + 1; Z_b^{\delta_{n-1}}), y^1 - y = v - y = (b - \lambda_n)/b^n$  and  $\delta_{n-1}(N_{n-1}) < \lambda_n < b$  (since Cases 1 and 2 are exclusive), which agrees with the definition of  $\varphi$ . And again, since  $b - \varepsilon_n = (\varphi_{b, \varepsilon_n}^{\delta_{n-1}})'(N/b^n)$ , we have  $\lambda^1 := y^1 b^{n-1} = (\lambda + (\varphi_{b, \varepsilon_n}^{\delta_{n-1}})'(N/b^n))/b$ , which ends Case 2.

For both cases, the first step ends with

$$E(y, N, X_n) = E(y^1, T_{n-1}, X_n) + \varphi_{b, \varepsilon_n}^{\delta_{n-1} \uplus \theta_{n-1}(N)}(N/b^n),$$

because  $E(y^1, N_{n-1}b^{n-1}, X_n) = A(y^1, N_{n-1}b^{n-1}, X_n) - y^1 N_{n-1}b^{n-1} = 0$  by the elementary interval property (indeed,  $A(y^1, N_{n-1}b^{n-1}, X_n) = \lambda^1 N_{n-1}$  since  $[0, y^1[$  is the union of  $\lambda^1$  elementary intervals of length  $b^{-n+1}$ ) and  $\theta_{n-1}(N) = 0$  from the definition of  $\theta$  (see 4.2).

If  $N = N_{n-1}b^{n-1}$ , we are done since  $T_{n-1} = T_{r_0}$  is empty and the functions  $\varphi$  vanish on the integers, which implies that the sum in the formula of Lemma 6.2 reduces to its last term.

SECOND STEP. This step is necessary only if  $N_{n-1}b^{n-1} < N < (N_{n-1} + 1)b^{n-1}$  (in which case  $N_{n-1} = a_{n-1}(N)$ ), that is, if  $x_N \in S_{n-1}$ ; in this situation, using the process of the first step, we write the remainder

$E(y^1, T_{n-1}, X_n)$  by means of the section  $S_{n-1}$  of  $X_n$  instead of  $]0, b^n]$  in the first step, the slice  $T_{n-1}$  taking the place of  $]0, N]$ .

First, we match up the formula for  $\eta_{n-1}$ :

$$\begin{aligned} \lambda^1 &= (\lambda + (\varphi_{b, \varepsilon_n}^{\delta_{n-1}})'(N/b^n))/b \\ &= \lambda_1 b^{n-2} + \dots + \lambda_{n-2} b + \lambda_{n-1} + \frac{\lambda_n}{b} + \frac{(\varphi_{b, \varepsilon_n}^{\delta_{n-1}})'(N/b^n)}{b}, \end{aligned}$$

that is,

$$\lambda^1 = \sum_{i=1}^{n-2} \lambda_i b^{n-i-1} + \eta_{n-1} \quad \text{with} \quad \eta_{n-1} = \lambda_{n-1} \text{ or } \lambda_{n-1} + 1,$$

since  $\varepsilon_n = \eta_n = \lambda_n$  and the derivative is  $-\varepsilon_n$  or  $b - \varepsilon_n$ .

- If  $\eta_{n-1} = b$ , we have nothing to do to descend the second step because  $\lambda^1$  is already a multiple of  $b$ , i.e.  $]0, y^1[$  is already rough enough (see the foreword above); on the other hand, in this case  $\varepsilon_{n-1} = 0$ , and so  $\varphi_{b, \varepsilon_{n-1}}^{\delta_{n-2} \uplus \theta_{n-2}(N)}$  and its derivative are the null functions; therefore the formula

$$E(y^1, T_{n-1}, X_n) = E(y^2, T_{n-1}, X_n) + \varphi_{b, \varepsilon_{n-1}}^{\delta_{n-2} \uplus \theta_{n-2}(N)}(N/b^{n-1})$$

is trivially satisfied with

$$y^2 := y^1, \quad \lambda^2 := y^2 b^{n-2} = \frac{\lambda^1 + (\varphi_{b, \varepsilon_{n-1}}^{\delta_{n-2} \uplus \theta_{n-2}(N)})'(N/b^{n-1})}{b}.$$

- If  $\eta_{n-1} < b$ , so that  $\varepsilon_{n-1} = \eta_{n-1}$ , we apply the process of the first step to  $y^1 \in \bar{Y}_{n-1}$  and to the section  $S_{n-1}$  of  $X_n$ : there exist unique  $u, v$  such that  $u \in \bar{Y}_{n-2}$ ,  $v = u + 1/b^{n-2}$  and  $u \leq y^1 < v$ ; according to Property 5.3 with  $s = 2$ , there exists a unique index  $i$  such that  $1 \leq i \leq b^{n-2}$  and  $x_{i+N_{n-2}b^{n-2}+N_{n-1}b^{n-1}} \in [u, v[$ ; to get it we should solve the system (\*\*) with  $\mu = \delta_{n-2}(N_{n-2}) + c_{n-2}^{n-1}N_{n-1} \pmod{b}$ , but once again, we do not need to know that  $i$ , as shown below in the two cases corresponding to those of the first step.

CASE 1. If  $y^1 \leq x_{i+N_{n-2}b^{n-2}+N_{n-1}b^{n-1}}$  then with  $y^2 := u$  we have

$$\begin{aligned} E(y^1, T_{n-1}, X_n) &= E(y^2, T_{n-1}, X_n) + A([y^2, y^1]; T_{n-1}; X_n) \\ &\quad - (N - N_{n-1}b^{n-1})(y^1 - y^2). \end{aligned}$$

From Property 5.3, the order of the terms of  $S_{n-1}$  in  $[u, v[$  is the same as the order of the terms of  $Z_b^{\sigma_{n-2}}$  in  $[0, 1[$  with  $\sigma_{n-2} = \delta_{n-2} \uplus c_{n-2}^{n-1}N_{n-1}$ , so that

$$A([y^2, y^1]; T_{n-1}; X_n) = A(\eta_{n-1}/b, N_{n-2} + 1, Z_b^{\sigma_{n-2}});$$

on the other hand, since  $y^1 = y^2 + \eta_{n-1}b^{-n+1}$ , we have

$$(N - N_{n-1}b^{n-1})(y^1 - y^2) = \frac{N - N_{n-1}b^{n-1}}{b^{n-1}} \eta_{n-1}$$

and

$$0 \leq \eta_{n-1} \leq \delta_{n-2}(N_{n-2}) + c_{n-2}^{n-1}N_{n-1} = \sigma_{n-2}(N_{n-2})$$

because

$$\begin{aligned} y^1 &\leq x_{i+N_{n-2}b^{n-2}+N_{n-1}b^{n-1}} \\ &= y^2 + \frac{\delta_{n-2}(N_{n-2}) + c_{n-2}^{n-1}N_{n-1}}{b^{n-1}} + \frac{\delta_{n-1}(N_{n-1})}{b^n}. \end{aligned}$$

Then, according to the definition of the  $\varphi$ 's, which are 1-periodic, we get (remember that here  $\varepsilon_{n-1} = \eta_{n-1}$  and  $N_{n-1} = a_{n-1}(N)$ )

$$A([y^2, y^1]; T_{n-1}; X_n) - (N - N_{n-1}b^{n-1})(y^1 - y^2) = \varphi_{b, \varepsilon_{n-1}}^{\delta_{n-2} \uplus \theta_{n-2}(N)}(N/b^{n-1}),$$

hence

$$E(y^1, T_{n-1}, X_n) = E(y^2, T_{n-1}, X_n) + \varphi_{b, \varepsilon_{n-1}}^{\delta_{n-2} \uplus \theta_{n-2}(N)}(N/b^{n-1}).$$

Moreover

$$\lambda^2 := y^2b^{n-2} = y^1b^{n-2} - \varepsilon_{n-1}/b = (\lambda^1 + (\varphi_{b, \varepsilon_{n-1}}^{\delta_{n-2} \uplus \theta_{n-2}(N)})'(N/b^{n-1}))/b$$

since the derivative is equal to  $-\varepsilon_{n-1}$ .

CASE 2. If  $y^1 > x_{i+N_{n-2}b^{n-2}+N_{n-1}b^{n-1}}$  then with  $y^2 := v$  we have

$$\begin{aligned} E(y^1, T_{n-1}, X_n) &= E(y^2, T_{n-1}, X_n) \\ &\quad - A([y^1, y^2]; T_{n-1}; X_n) + (N - N_{n-1}b^{n-1})(y^2 - y^1) \end{aligned}$$

and, for the same reason as in Case 1, we obtain

$$A([y^1, y^2]; T_{n-1}; X_n) = A([\eta_{n-1}/b, 1]; N_{n-2} + 1; Z_b^{\sigma_{n-2}})$$

and

$$(N - N_{n-1}b^{n-1})(y^2 - y^1) = \frac{N - N_{n-1}b^{n-1}}{b^{n-1}}(b - \eta_{n-1})$$

because  $y^2 - y^1 = b^{-n+2} - \eta_{n-1}b^{-n+1}$ ; so that, still with  $\varepsilon_{n-1} = \eta_{n-1}$  and  $N_{n-1} = a_{n-1}(N)$ , we have

$$-A([y^1, y^2]; T_{n-1}; X_n) + (N - N_{n-1}b^{n-1})(y^2 - y^1) = \varphi_{b, \varepsilon_{n-1}}^{\delta_{n-2} \uplus \theta_{n-2}(N)}(N/b^{n-1})$$

(again here  $\delta_{n-2}(N_{n-2}) + c_{n-2}^{n-1}N_{n-1} < \eta_{n-1} < b$  since Cases 1 and 2 are exclusive). Thus

$$E(y^1, T_{n-1}, X_n) = E(y^2, T_{n-1}, X_n) + \varphi_{b, \varepsilon_{n-1}}^{\delta_{n-2} \uplus \theta_{n-2}(N)}(N/b^{n-1})$$

and

$$\lambda^2 := y^2b^{n-2} = y^1b^{n-2} + 1 - \varepsilon_{n-1}/b = (\lambda^1 + (\varphi_{b, \varepsilon_{n-1}}^{\delta_{n-2} \uplus \theta_{n-2}(N)})'(N/b^{n-1}))/b$$

since the derivative is equal to  $b - \varepsilon_{n-1}$ ; this ends the Case 2 of the second step.

Now, to end the second step, we note that

$$E(y^2; ]N_{n-1}b^{n-1}, N_{n-1}b^{n-1} + N_{n-2}b^{n-2}]; X_n) = 0$$

by the elementary interval property (as for the first step), so that

$$E(y^2, T_{n-1}, X_n) = E(y^2, T_{n-2}, X_n)$$

and

$$\begin{aligned} E(y, N, X_n) &= E(y^2, T_{n-2}, X_n) \\ &\quad + \varphi_{b, \varepsilon_{n-1}}^{\delta_{n-2} \uplus \theta_{n-2}(N)}(N/b^{n-1}) + \varphi_{b, \varepsilon_n}^{\delta_{n-1} \uplus \theta_{n-1}(N)}(N/b^n). \end{aligned}$$

If  $N = N_{n-1}b^{n-1} + N_{n-2}b^{n-2}$ , we have the desired formula (in which the sum has two terms only) since  $r_0 = n - 2$ , which implies  $T_{n-2}$  is empty, and since the functions  $\varphi$  vanish on the integers.

*Iteration.* If  $x_N \in S_{n-2}$ , we begin the third step by first bringing out  $\eta_{n-2}$  from the  $b$ -adic expansion of  $\lambda^2$ :

$$\begin{aligned} \lambda^2 &= (\lambda^1 + (\varphi_{b, \varepsilon_{n-1}}^{\delta_{n-2} \uplus \theta_{n-2}(N)})'(N/b^{n-1}))/b \\ &= \sum_{i=1}^{n-3} \lambda_i b^{n-i-2} + \lambda_{n-2} + \frac{\eta_{n-1}}{b} + \frac{(\varphi_{b, \varepsilon_{n-1}}^{\delta_{n-2} \uplus \theta_{n-2}(N)})'(N/b^n)}{b}, \end{aligned}$$

which shows that  $\eta_{n-2} = \lambda_{n-2}$  or  $\lambda_{n-2} + 1$  (since the derivative is  $-\varepsilon_{n-1} = -\eta_{n-1}$  or  $b - \varepsilon_{n-1} = b - \eta_{n-1}$  or 0 if  $\eta_{n-1} = b$ ). Then if  $\eta_{n-2} = b$ , the third step is void, and else we apply the descent process to  $y^2 \in \bar{Y}_{n-2}$  and to  $S_{n-2}$  which involves the antepenultimate row of the matrix of (\*) and leads to

$$E(y, N, X_n) = E(y^3, T_{n-3}, X_n) + \sum_{j=n-2}^n \varphi_{b, \varepsilon_j}^{\delta_{j-1} \uplus \theta_{j-1}(N)}(N/b^j).$$

Continuing in that way, we get the desired formula since, along the descent, the process still ends as in the first and second steps, except if  $r_0 = 0$ , in which case we have to perform the last step, step  $s = n$ , in order to express  $E(y^{n-1}, T_1, X_n)$  when  $x_N \in S_1$ .

From step  $n - 1$ , by recursion hypothesis we have

$$\lambda^{n-1} := y^{n-1}b = (\lambda^{n-2} + (\varphi_{b, \varepsilon_2}^{\delta_1 \uplus \theta_1(N)})'(N/b^2))/b \quad \text{with} \quad \lambda^{n-2} = \lambda_1 b + \eta_2,$$

so that

$$\lambda^{n-1} = \lambda_1 + \frac{\eta_2}{b} + \frac{(\varphi_{b, \varepsilon_2}^{\delta_1 \uplus \theta_1(N)})'(N/b^2)}{b} = \eta_1.$$

- If  $\eta_1 = b$ , the step  $n$  is void:  $E(y^{n-1}, T_1, X_n) = E(\eta_1/b, T_1, X_n) = 0$ .
- If  $\eta_1 < b$ , we apply once more the descent process, now to  $y^{n-1} \in \bar{Y}_1$  and  $S_1$ : there exist unique  $u, v$  such that  $u \in \bar{Y}_0 = \{0\}$ ,  $v = u + b^{-n+s} = 1$

and  $u \leq y^{n-1} < v$ ; according to Property 5.3 with  $s = n$ , there exists a unique  $i$  such that  $1 \leq i \leq b^0$  (thus here we get  $i = 1$ ) and

$$x_{i+\sum_{k=0}^{n-1} N_k b^k} = x_{N+1} \in [0, 1[.$$

The unique equation of  $(**)$ ,  $\delta_0(a_0) + \sum_{k=1}^{n-1} c_0^k N_k = \mu$ , shows that the order of the terms of  $S_1$  in  $[0, 1[$  is the same as the order of the terms of  $Z_b^{\sigma_0}$  in  $[0, 1[$ , with  $\sigma_0 = \delta_0 \uplus \sum_{k=1}^{n-1} c_0^k N_k = \delta_0 + \theta_0(N)$  (here  $N_k = a_k(N)$  for all  $k \geq 1$  since  $r_0 = 0$ ).

Then the two cases corresponding to  $y^{n-1}$  less or greater than  $x_{N+1}$  lead, still in the same way, to

$$E(y^{n-1}, T_1, X_n) = E(y^n, T_1, X_n) + \varphi_{b, \varepsilon_1}^{\delta_0 \uplus \theta_0(N)}(N/b)$$

with  $y^n = 0$  or  $1$ , so that  $E(y^n, T_1, X_n) = 0$ , and the proof of Lemma 6.2 is complete. ■

**6.3. LEMMA** (values of the  $\varepsilon_j$ 's). *With the notations of Lemma 6.2 and with  $\sigma_r = \delta_r \uplus \theta_r(N)$ , for  $0 \leq j \leq n - 1$  set*

$$\Lambda_j = \sum_{r=j+1}^n \lambda_r b^{n-r}, \quad \nu_j = \sum_{r=j}^{n-1} \sigma_r(N_r) b^{n-r-1} \quad (\text{with } N_r = 0 \text{ if } r < r_0).$$

Then, for  $1 \leq j \leq n - 1$ , we have

$$\eta_j = \begin{cases} \lambda_j & \text{if } 0 \leq \Lambda_j \leq \nu_j, \\ \lambda_j + 1 & \text{if } \nu_j < \Lambda_j < b^{n-j}, \end{cases}$$

and

$$\varepsilon_j = \begin{cases} 0 & \text{if } 0 \leq \Lambda_{j-1} \leq \nu_j, \\ p & \text{if } \nu_j + (p - 1)b^{n-j} < \Lambda_{j-1} \leq \nu_j + pb^{n-j} \text{ (for } 1 \leq p < b), \\ 0 & \text{if } \nu_j + (b - 1)b^{n-j} < \Lambda_{j-1} < b^{n-j+1}. \end{cases}$$

*Proof.* It is identical with the proof of Lemma 5.3 of [2], but with a fixed base instead of variable bases; for the sake of completeness, we point out the guidelines:

First, the results are still valid for  $j = n$  with the convention  $\Lambda_n = \nu_n = 0$ , since then  $\Lambda_{n-1} = \lambda_n$ .

Next, the formulas for  $\eta_j$  are proven by recursion in the special case of the identical permutation  $I$ , first for the rank  $j = n - 1$  by using the definition of  $\eta_{n-1}$  (Lemma 6.2) and of the function  $\varphi_{b, \varepsilon_n}^I$ , and then for the rank  $j$  assuming they are true for the rank  $j + 1$ : in the case where  $0 \leq \Lambda_j \leq \nu_j$ , there are two subcases corresponding to  $\Lambda_{j+1} \leq \nu_{j+1}$  and  $\Lambda_{j+1} > \nu_{j+1}$ , but each of them gives  $\eta_j = \lambda_j$  because  $\eta_{j+1} + (\varphi_{b, \varepsilon_{j+1}}^I)'(N/b^{j+1}) = 0$  for both; the other case, where  $\nu_j < \Lambda_j < b^{n-j}$ , is handled in the same way.

Now, in the general situation with arbitrary permutations  $\sigma_r$ , the results for the  $\eta_j$ 's are obtained with the help of Property 3.0 which asserts that

$$(\varphi_{b,\varepsilon_{r+1}}^{\sigma_r})'(N/b^{r+1}) = (\varphi_{b,\varepsilon_{r+1}}^{\sigma_r})'(N_r/b) = (\varphi_{b,\varepsilon_{r+1}}^I)'(\sigma_r(N_r)/b),$$

so that we are brought back to the special case of  $I$  with

$$N' = \sum_{r=j}^{n-1} \sigma_r(N_r)b^r, \quad \nu'_j = \sum_{r=j}^{n-1} I(\sigma_r(N_r))b^{n-r-1} = \nu_j.$$

Finally, the formulas for the  $\varepsilon_j$ 's are deduced from those for the  $\eta_j$ 's by enumeration of the different cases. ■

**6.4. Proof of Theorem 1.** It works on the same principle as that of Theorem 1 in [3] but the development is different and simpler because in [3] we did not have an exact formula for the remainder like that of Lemma 6.2, with the good control of the  $\varepsilon_j$ 's by Lemma 6.3.

In the following,  $N \geq 1$  is a fixed integer and  $n$  is any integer satisfying  $N \leq b^n$ . We only prove the formula for  $D^+$ , the one for  $D^-$  being obtained in the same way.

First, with the discretization Lemma 6.1, we get

$$\lim_{n \rightarrow \infty} (\sup_{y \in \bar{Y}_n} E(y, N, X_b^C)) = D^+(N, X_b^C)$$

(for a detailed proof, see [3, Lemma 3.3.1] with  $\bar{X}_n = \bar{Y}_n$ ).

Next, the descent Lemma 6.2 implies that, for all  $y = \lambda/b^n \in \bar{Y}_n$ ,

$$E(y, N, X_b^C) \leq \sum_{j=1}^n \psi_b^{\sigma_{j-1},+}(N/b^j)$$

with  $\sigma_{j-1} = \delta_{j-1} \uplus \theta_{j-1}(N)$ .

Finally, in the following, we show this upper bound is reached by some  $y \in \bar{Y}_n$ . For  $1 \leq j \leq n$ , let  $p_j$  ( $0 \leq p_j < b$ ) be an integer such that  $\psi_b^{\sigma_{j-1},+}(N/b^j) = \varphi_{b,p_j}^{\sigma_{j-1}}(N/b^j)$ , so that we have a fixed sequence  $\varepsilon_j = p_j$  from which we can deduce an integer  $\lambda = \lambda_1 b^{n-1} + \dots + \lambda_n$  satisfying

$$E(\lambda b^{-n}, N, X_b^C) = \sum_{j=1}^n \varphi_{b,p_j}^{\sigma_{j-1}}(N b^{-j}) = \sum_{j=1}^n \psi_b^{\sigma_{j-1},+}(N b^{-j});$$

indeed, using the formulas of Lemma 6.2 for  $\eta_j$  and  $\varepsilon_j$ , we build  $\lambda$  step by step, first by setting  $\lambda_n := \eta_n := p_n$  and then, if  $\eta_j$  and  $\lambda_j$  are achieved, by using the reverse algorithm (of the construction of the  $\varepsilon_j$  from the  $\lambda_j$ ):

if  $\frac{\eta_j}{b} + \frac{1}{b}(\varphi_{b,p_j}^{\sigma_{j-1}})'(N b^{-j}) = 0$  then  $\lambda_{j-1} := \eta_{j-1} := p_{j-1}$

else (i.e. if  $\frac{\eta_j}{b} + \frac{1}{b}(\varphi_{b,p_j}^{\sigma_{j-1}})'(N b^{-j}) = 1$ )

if  $p_{j-1} \geq 1$  then  $\eta_{j-1} := p_{j-1}$  and  $\lambda_{j-1} := \eta_{j-1} - 1$   
 else (i.e. if  $p_{j-1} = 0$ )  $\eta_{j-1} := b$  and  $\lambda_{j-1} := \eta_{j-1} - 1$ ;

the algorithm ends when  $j = r_0 + 1$  (see the notations of Lemma 6.2); this means that we have exactly  $b^{r_0}$  values of  $\lambda$  for which the above upper bound is reached.

The end of the proof of Theorem 1 is straightforward by letting  $n \rightarrow \infty$ . ■

REMARK. This proof gives the reals  $\alpha \in [0, 1[$  for which the discrepancy  $D^+$  is reached, as well as that for  $D^-$ , for both  $X_b^C$  and  $S_b^\Sigma$  (by using Lemma 5.2 of [2] for the last one); explicit computations of these  $\alpha$  could be made to obtain formulas like those we obtained in [1] for the initial van der Corput sequence in base 2 (remember that, in this case, we have  $D = D^* = D^+$  and  $D^- = 0$ ).

**6.5. Proof of Theorem 3.** Here, the proof is parallel to the analogous one of [2, Theorem 4.1], but it is simpler for two reasons: first we work with a fixed base and then our sequences  $X_b^C$  begin with  $x_1 = 0$  unlike the  $S_b^\Sigma$  which begin with  $x_1 = \sum_{r=0}^\infty \sigma_r(a_r(1))/b^{r+1}$ . We give the outline with these simplifications and emphasize the leading part of Lemma 6.3 in the appearance of the functions  $\varphi_b^\sigma$  and  $\phi_b^\sigma$ .

First, we write  $E(\alpha, N) := E(\alpha, N, X_b^C)$  and compute the  $L_2$ -discrepancy  $T^2(N) = \int_0^1 E^2(\alpha, N) d\alpha$  by using Lemma 6.1. For  $1 \leq \lambda \leq b^n$  and  $\alpha \in [(\lambda - 1)b^{-n}, \lambda b^{-n}[$ , we have

$$E(\alpha, N) = \begin{cases} E(\lambda b^{-n}, N) + (\lambda b^{-n} - \alpha)N & \text{if } (\lambda - 1)b^{-n} < \alpha, \\ E((\lambda - 1)b^{-n}, N) & \text{if } (\lambda - 1)b^{-n} = \alpha, \end{cases}$$

so that, after computation,

$$\int_0^1 E^2(\alpha, N) d\alpha = \frac{1}{b^n} \sum_{\lambda=1}^{b^n} E^2(\lambda b^{-n}, N) + \frac{N}{b^{2n}} \sum_{\lambda=1}^{b^n} E(\lambda b^{-n}, N) + \frac{N^2}{3b^{2n}}.$$

Next, applying Lemma 6.2 with  $\sigma_{j-1} = \delta_{j-1} \uplus \theta_{j-1}(N)$ , we get successively

$$\begin{aligned} A &:= \sum_{\lambda=1}^{b^n} E(\lambda b^{-n}, N) = \sum_{j=1}^n \sum_{\lambda=1}^{b^n} \varphi_{b, \varepsilon_j}^{\sigma_{j-1}}(Nb^{-j}), \\ B &:= \sum_{\lambda=1}^{b^n} E^2(\lambda b^{-n}, N) \\ &= \sum_{j=1}^n \sum_{\lambda=1}^{b^n} (\varphi_{b, \varepsilon_j}^{\sigma_{j-1}})^2(Nb^{-j}) + 2 \sum_{1 \leq i < j \leq n} \sum_{\lambda=1}^{b^n} \varphi_{b, \varepsilon_i}^{\sigma_{i-1}}(Nb^{-i}) \varphi_{b, \varepsilon_j}^{\sigma_{j-1}}(Nb^{-j}) \end{aligned}$$

in which (remember again) the  $\varepsilon_j$ 's are functions of  $\lambda$  and  $N$ .

For a fixed  $j$ , since  $\lambda = \lambda_1 b^{n-1} + \dots + \lambda_{j-1} b^{n-j+1} + \Lambda_{j-1}$ , the set of  $\lambda$ 's is divided into  $b^{n-j+1}$  classes, each with  $b^{j-1}$  elements, where  $\Lambda_{j-1}$  is constant; thus, from Lemma 6.3, we get  $\varepsilon_j(\lambda) = p$  for  $b^{n-1}$  values of  $\lambda$ . Therefore,

$$A = \sum_{j=1}^n \left( b^{n-1} \sum_{p=0}^{b-1} \varphi_{b,p}^{\sigma_{j-1}}(Nb^{-j}) \right) = b^{n-1} \sum_{j=1}^n \varphi_b^{\sigma_{j-1}}(Nb^{-j})$$

and similarly

$$\sum_{j=1}^n \sum_{\lambda=1}^{b^n} (\varphi_{b,\varepsilon_j}^{\sigma_{j-1}})^2(Nb^{-j}) = b^{n-1} \sum_{j=1}^n \phi_b^{\sigma_{j-1}}(Nb^{-j}).$$

The second part of  $B$  requires a further analysis: for fixed  $i$  and  $j$ , each class above is itself divided into  $b^{j-1-i}$  subclasses with  $b^{i-1}$  elements each, where  $\Lambda_{i-1}$  is constant; thus for all  $p$  and  $q$ , we have  $\varepsilon_j(\lambda) = p$  and  $\varepsilon_i(\lambda) = q$  for  $b^{n-2}$  values of  $\lambda$ ; in the end, we get

$$B = b^{n-1} \sum_{j=1}^n \phi_b^{\sigma_{j-1}}(Nb^{-j}) + 2b^{n-2} \sum_{1 \leq i < j \leq n} \varphi_b^{\sigma_{i-1}}(Nb^{-i}) \varphi_b^{\sigma_{j-1}}(Nb^{-j}).$$

Finally, carrying back  $A$  and  $B$  into the integral, we obtain Theorem 3 by letting  $n \rightarrow \infty$  with fixed  $N$ : indeed,  $|A| \leq nb^{n+1}/4$  since  $|\varphi_b^\sigma| \leq b^2/4$  (Property 3.0), so that the two last summands in the integral have a null limit. ■

**6.6. Proofs of Theorems 2 and 4.** The main argument is the same for both theorems; this is the reason why we gather together the proofs. Before giving it in the proposition below, we prepare the formulas for  $D$  and  $F$ .

From the relations  $D = D^+ + D^-$  and  $\psi_b^\sigma = \psi_b^{\sigma,+} + \psi_b^{\sigma,-}$ , we deduce immediately from Theorem 1 that

$$D(N, X_b^C) = \sum_{j=1}^{\infty} \psi_b^{\delta_{j-1} \uplus \theta_{j-1}(N)}(Nb^{-j}).$$

Concerning  $F$ , we apply the formula of Koksma and Theorem 3: using the method of 6.5, it is easy to compute  $\int_0^1 E(\alpha, N) d\alpha$  with the help of the quantity  $A$ , so that

$$\int_0^1 E(\alpha, N) d\alpha = \frac{1}{b} \sum_{j=1}^n \varphi_b^{\sigma_{j-1}}(Nb^{-j}) + \frac{N}{2b^n}.$$

Therefore, using the computation for  $T^2$  and letting  $n \rightarrow \infty$ , we obtain

$$\begin{aligned}
 (2\pi)^{-2}F^2(N, X_b^C) &= T^2(N, X_b^C) - \left( \int_0^1 E(\alpha, N) d\alpha \right)^2 \\
 &= \sum_{j=1}^{\infty} \left( \frac{1}{b} \phi_b^{\sigma_{j-1}} - \frac{1}{b^2} (\varphi_b^{\sigma_{j-1}})^2 \right) (Nb^{-j}) \\
 &= \frac{1}{b^2} \sum_{j=1}^{\infty} \chi_b^{\sigma_{j-1}} (Nb^{-j}),
 \end{aligned}$$

of course with  $\sigma_{j-1} = \delta_{j-1} \uplus \theta_{j-1}(N)$ .

Now, we claim that the translation of  $\delta$  by  $\theta$  does not affect  $D$  and  $F$  because of the special nature of  $\psi$  and  $\chi$ , according to the following proposition:

**PROPOSITION.** *Let  $\sigma$  be a permutation of  $\mathbb{F}_b$  and  $t$  an element of  $\mathbb{F}_b$ . Then*

$$\psi_b^{\sigma \uplus t} = \psi_b^{\sigma}, \quad \chi_b^{\sigma \uplus t} = \chi_b^{\sigma}.$$

*Proof.* First, according to the formulas

$$\psi_b^{\sigma} = \max_{0 \leq h < h' \leq b-1} |\varphi_{b,h}^{\sigma} - \varphi_{b,h'}^{\sigma}|, \quad \chi_b^{\sigma} = \sum_{0 \leq h < h' \leq b-1} (\varphi_{b,h}^{\sigma} - \varphi_{b,h'}^{\sigma})^2$$

(end of 4.1), we need only verify that the set of differences  $\varphi_{b,h} - \varphi_{b,h'}$  is the same for  $\sigma$  and  $\sigma \uplus t$ ; and since the translation  $(t, t)$  is a permutation of  $\mathbb{F}_b^2$ , this amounts to proving that  $\varphi_{b,h}^{\sigma} - \varphi_{b,h'}^{\sigma} = \varphi_{b,h+t}^{\sigma \uplus t} - \varphi_{b,h'+t}^{\sigma \uplus t}$  for all  $h$  and  $h'$  (in which, of course,  $h+t$  and  $h'+t$  are mod  $b$ ).

Next, remember the functions are continuous and piecewise affine, so it is enough to check that

$$\varphi_{b,h}^{\sigma}(k/b) - \varphi_{b,h'}^{\sigma}(k/b) = \varphi_{b,h+t}^{\sigma \uplus t}(k/b) - \varphi_{b,h'+t}^{\sigma \uplus t}(k/b)$$

for all  $h, h'$  and  $k$  ( $1 \leq k \leq b$ ). Coming back to the definition of  $\varphi_{b,h}$ , this is equivalent to

$$E(h/b, k, Z_b^{\sigma}) - E(h'/b, k, Z_b^{\sigma}) = E((h+t)/b, k, Z_b^{\sigma \uplus t}) - E((h'+t)/b, k, Z_b^{\sigma \uplus t}),$$

i.e.

$$E\left(\left[\frac{h}{b}, \frac{h'}{b}\right]; k; Z_b^{\sigma}\right) = E\left(\left[\frac{h+t}{b}, \frac{h'+t}{b}\right]; k; Z_b^{\sigma \uplus t}\right),$$

which is obvious since the interval and the set of points are translated by the same quantity. ■

This proposition completes the proof of Theorems 2 and 4. ■

**6.7. Proof of the Corollary.** For  $D^+$ ,  $D^-$ ,  $D$ , and  $F$ , it is a direct consequence of the knowledge of the functions  $\psi_b^{\sigma,+}$ ,  $\psi_b^{\sigma,-}$ ,  $\psi_b^{\sigma}$  and  $\chi_b^{\sigma}$  on the

interval  $[0, 1/b]$ :

$$\begin{aligned} \psi_b^{\sigma,+}(x) &= (b - \sigma(0) - 1)x, & \psi_b^{\sigma,-}(x) &= \sigma(0)x, \\ \psi_b^\sigma(x) &= (b - 1)x, & \chi_b^\sigma(x) &= \frac{b^2(b^2 - 1)x^2}{12} \end{aligned}$$

([3, Property 3.2.1(ii)] and [2, Property 3.5(ii)]); indeed, remember that  $\sigma_r = \delta_r$  for all  $r \geq n - 1$  (see 4.2) and that  $\delta_r(0) = 0$  since  $\delta_r$  is the multiplication with  $c_r^r$ ; therefore the end of the sum from  $n + 1$  to infinity is geometric in each case and the formulas follow.

Concerning  $T$ , we use the formula of Koksma with the formula we just got for the diaphony and the expression we got for  $\int_0^1 E(\alpha, N) d\alpha$  in 6.6, so that we obtain the desired result without any geometric summation:

$$T^2(N, X_b^C) = \left( \frac{1}{b} \sum_{j=1}^n \varphi_b^{\sigma_{j-1}} \left( \frac{N}{bj} \right) + \frac{N}{2b^n} \right)^2 + \frac{1}{b^2} \sum_{j=1}^n \chi_b^{\delta_{j-1}} \left( \frac{N}{bj} \right) + \frac{N^2}{12b^{2n}}. \blacksquare$$

As a consequence of this Corollary, letting  $n \rightarrow \infty$  with fixed  $N$ , we obtain the following asymptotic formula for the  $L_2$ -discrepancy of  $X_b^C$ , the same we got for  $S_b^{\mathcal{Z}}$  in [2, 4.2.1, Remark 3], since the order of the diaphony is  $O(\sqrt{\log N})$ :

$$T^2(N, X_b^C) = \frac{1}{b^2} \left( \sum_{j=1}^{\infty} \varphi_b^{\delta_{j-1} \uplus \theta_{j-1}(N)} \left( \frac{N}{bj} \right) \right)^2 + O(\log N).$$

Therefore, the asymptotic behaviour of  $T(N, X_b^C)$  is directly linked to the properties of the functions  $\varphi_b^{\delta_{j-1} \uplus \theta_{j-1}(N)}$ .

### References

- [1] R. Bélian et H. Faure, *Discr pance de la suite de van der Corput*, C. R. Acad. Sci. Paris S r. A 285 (1977), 313–316 and S minaire Delange–Pisot–Poitou, 19 me ann e 1977/78, Exp. 13 (1978), 14 p.
- [2] H. Chaix et H. Faure, *Discr pance et diaphonie en dimension un*, Acta Arith. 63 (1993), 103–141.
- [3] H. Faure, *Discr pance de suites associ es   un syst me de num ration (en dimension un)*, Bull. Soc. Math. France 109 (1981), 143–182.
- [4] —, *Discr pance de suites associ es   un syst me de num ration (en dimension s)*, Acta Arith. 41 (1982), 337–351.
- [5] —, *Good permutations for extreme discrepancy*, J. Number Theory 42 (1992), 47–56.
- [6] V. S. Grozdanov, *On the diaphony of one class of one-dimensional sequences*, Internat. J. Math. Math. Sci. 19 (1996), 115–124.
- [7] L. Kuipers and H. Niederreiter, *Uniform Distribution of Sequences*, Wiley, New York, 1974.
- [8] G. Larcher and F. Pillichshammer, *Walsh series analysis of the  $L_2$ -discrepancy of symmetrized point sets*, Monatsh. Math. 132 (2001), 1–18.

- [9] G. Larcher and F. Pillichshammer, *Sums of distances to the nearest integer and the discrepancy of digital nets*, Acta Arith. 106 (2003), 379–408.
- [10] H. Niederreiter, *Point sets and sequences with small discrepancy*, Monatsh. Math. 104 (1987), 273–337.
- [11] —, *Random Number Generation and Quasi-Monte Carlo Methods*, CBMS-NSF Regional Conf. Ser. in Appl. Math. 63, SIAM, 1992.
- [12] F. Pillichshammer, *On the discrepancy of  $(0, 1)$ -sequences*, J. Number Theory 104 (2004), 301–314.

Institut de Mathématiques de Luminy  
U.P.R. 9016 CNRS  
Case 907  
163 avenue de Luminy  
F-13288 Marseille Cedex 09, France  
E-mail: faure@iml.univ-mrs.fr

*Received on 7.5.2004  
and in revised form on 4.9.2004*

(4761)