Best possible lower bounds for the star discrepancy of (0,1)-sequences

Henri Faure (with Friedrich Pillichshammer)

Institut de mathématiques de Luminy - CNRS, Marseille, France

faure@iml.univ-mrs.fr

UDT 2012, June 24th to 29th, Smolenice Slovakia

Outline

Discrepancies

For an infinite sequence $X = (x_n)_{n\geq 1}$ in $[0,1]$, a sub-interval $[\alpha,\beta)$ of $[0,1]$, and an integer $N \geq 1$, the discrepancy function is the difference

$$E([\alpha,\beta);N;X) = A([\alpha,\beta);N;X) - N(\beta-\alpha), \text{where}$$

$A(J,N) = \#\{n; 1 \leq n \leq N, X_n \in J\}$. Various discrepancies of X:

$$D(N,X) = \sup_{0\leq\alpha<\beta\leq 1} |E([\alpha,\beta);N;X)|,\ D^*(N,X) = \sup_{0\leq\alpha\leq 1} |E([0,\alpha);N;X)|,$$

$$D^+(N,X) = \sup_{0\leq\alpha\leq 1} E([0,\alpha);N;X),\ D^-(N,X) = \sup_{0\leq\alpha\leq 1} (-E([0,\alpha);N;X)).$$

We have $D = D^+ + D^-, \quad D^* = \max(D^+,D^-)$ and $D^* \leq D \leq 2D^*$.

Sequences
1. Generalized van der Corput sequences

Let $b \geq 2$ be an arbitrary integer and let $\Sigma = (\sigma_r)_{r\geq 0}$ be a sequence of permutations of $\{0, 1, \ldots, b-1\}$. For any integer $N \geq 1$, the generalized van der Corput sequence S_b^Σ in base b associated with Σ is defined by

$$S_b^\Sigma(N) = \sum_{r=0}^{\infty} \frac{\sigma_r\Big(a_r(N)\Big)}{b^{r+1}}, \text{ with } N-1 = \sum_{r=0}^{\infty} a_r(N)\ b^r,$$

(b-adic expansion of $N-1$).

If $\Sigma = (\sigma_r) = (\sigma)$ is constant, we write $S_b^\Sigma = S_b^\sigma$.

van der Corput sequences in base b, S_b^{id}, are obtained with identical permutations id. The original van der Corput sequence (1935) is S_2^{id}.

2. Digital (0,1) sequences over $\mathbb{Z}_b$

Instead of permutations, infinite matrices over $\mathbb{Z}_b$ act on the digits:

Let $C = (c_k^r)_{r\geq 0, k\geq 0}$ be an infinite matrix with $c_k^r \in \mathbb{Z}_b$ such that every left upper sub-matrix of C is non singular.

Then a digital (0,1)-sequence X_b^C associated with C is defined by

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

Note that the second summation is finite and performed in $\mathbb{Z}_b$, but the first one can be infinite with the possibility that $x_{N,r} = b-1$ for all but finitely many r (hence requiring a troncation operator as defined by Niederreiter–Xing (1995)).

Remark: Generalized van der Corput sequences and digital (0,1)-sequences are (0,1)-sequences in the sense of Niederreiter–Xing.

3. NUT digital (0,1)-sequences over $\mathbb{Z}_b$

Are sequences X_b^C with nonsingular upper triangular C. Formulas have been proved for D^+ and D^- (HF'05) needing more notations:

Let σ be a permutation of $\mathbb{Z}_b$ and set $Z_b^\sigma := \left(\frac{\sigma(0)}{b}, \cdots, \frac{\sigma(b-1)}{b}\right)$.

The so-called functions $\varphi_{b,h}^\sigma$ related to a pair (b,σ) are linearizations of discrepancy functions associated with Z_b^σ, defined on $[0,1]$, and then extended to $\mathbb{R}$ by periodicity: For any integers h,k with $0 \le h \le b-1$, $1 \le k \le b$ and any real x with $(k-1)/b \le x < k/b$ we set

$$\varphi_{b,h}^\sigma(x) = A\left(\left[0, \frac{h}{b}\right[; k; Z_b^\sigma\right) - hx \text{ if } 0 \le h \le \sigma(k-1) \quad \text{and}$$

$$\varphi_{b,h}^\sigma(x) = (b-h)x - A\left(\left[\frac{h}{b}, 1\right[; k; Z_b^\sigma\right) \text{ if } \sigma(k-1) < h < b.$$

Note that $\varphi_{b,0}^{\sigma} = 0$. The b functions $\varphi_{b,h}^{\sigma}$ give rise to other functions:

$\psi_b^{\sigma,+} = \max_{0 \le h \le b-1} (\varphi_{b,h}^{\sigma}),\ \psi_b^{\sigma,-} = \max_{0 \le h \le b-1} (-\varphi_{b,h}^{\sigma})$ and $\psi_b^{\sigma} = \psi_b^{\sigma,+} + \psi_b^{\sigma,-}$

which appear in formulas below for D^+, D^- and D. Further set

$$\theta_r(N) := \sum_{k=r+1}^{\infty} c_r^k a_k(N) \,(\mathrm{mod}\, b) \quad (r \ge 0).$$

Moreover, with the diagonal entries c_r^r of C, define permutations δ_r by $\delta_r(i) := c_r^r i\,(\mathrm{\ mod\ } b)$. And finally, define the translated permutation of a given permutation σ with a given $t \in \mathbb{Z}_b$ by

$$(\sigma \uplus t)(i) := \sigma(i) + t \,(\mathrm{mod}\, b) \text{ for all } i \in \mathbb{Z}_b.$$

Together, these definitions permit to state a theorem from (HF'05):

Theorem 1. Let b be a prime. For any NUT digital $(0,1)$-sequence X_b^C over $\mathbb{Z}_b$, we have

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

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

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

Remarks: In fact these series are geometrical for sufficiently large indices j ($j > n$ for integers n such that $1 \leq N \leq b^n$).
The most remarkable feature is that D, the extreme discrepancy, only depends on the diagonal entries of C, via permutations δ_r.
Similar formulas exist for L_2 discrepancy and diaphony.

4. Generalized NUT (0,1)-sequences over $\mathbb{Z}_b$

We now introduce a mixed construction for arbitrary bases containing generalized van der Corput sequences and NUT digital $(0,1)$-sequences over $\mathbb{Z}_b$. The idea is to put arbitrary permutations in place of the diagonal entries of C. Let $\mathfrak{S}_b$ be the set of permutations of $\mathbb{Z}_b$.

Definition: For any integer $b \geq 2$, let $\Sigma = (\sigma_r)_{r\geq 0} \in \mathfrak{S}_b^{\mathbb{N}}$ be a sequence of permutations and let $C = (c_r^k)_{r\geq 0, k\geq r+1}$ be a strict upper triangular (SUT) matrix with entries in $\mathbb{Z}_b$. Then, for all integers $N \geq 1$, set

$$X_b^{\Sigma,C}(N) = \sum_{r=0}^{\infty} \frac{x_{N,r}}{b^{r+1}} \text{ with } x_{N,r} = \sigma_r(a_r(N)) + \sum_{k=r+1}^{\infty} c_r^k a_k(N) \pmod{b}.$$

We call $X_b^{\Sigma,C}$ a NUT $(0,1)$-sequence over $\mathbb{Z}_b$.

Remark: If all entries of C are zero, then we have $X_b^{\Sigma,C} = S_b^{\Sigma}$, the generalized van der Corput sequence associated with Σ.
If $\sigma_r = \delta_r$ (multiplication by c_r^r) for all r, then we have $X_b^{\Sigma,C} = X_b^{C'}$, the NUT digital $(0,1)$-sequence with generating matrix $C' = (c_r^k)_{r\geq 0, k\geq r}$ obtained from C by putting entries c_r^r on the diagonal.
It is quite remarkable that Theorem 1 is still valid for $X_b^{\Sigma,C}$ sequences:

Theorem 2. For any NUT $(0,1)$-sequence $X_b^{\Sigma,C}$ over $\mathbb{Z}_b$, we have

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

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

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

The proof closely follows that of Theorem 1, but is rather complex and requires several technical changes.
Concerning QMC Methods, this extension enlarges the choices of "good" scramblings for the construction of efficient point sets which can avoid correlations induced by linear permutations.
Concerning Number Theory, as an application of Theorem 2, we are interested in this talk to obtain best possible lower bounds for the star discrepancy of many sub-classes of $(0,1)$-sequences in base b. In this way we generalize results on shifted van der Corput sequences in base 2 from Kritzer, Larcher and Pillichshammer to a wide extent.

Best possible lower bounds for star discrepancy

1.Overview of the problem

For an infinite sequence X in $[0,1]$, set

$$s(X) := \limsup_{N\to\infty} \frac{D(N,X)}{\log N} \quad \text{and} \quad s^*(X) := \limsup_{N\to\infty} \frac{D^*(N,X)}{\log N}.$$

A famous theorem of Schmidt (72 further improved by Béjian 82) states that for any X, $s(X) > 0.12$, and hence $s^*(X) > 0.06$.

On the other hand, it is known that this order is best possible with $s^*(S_2^{\text{id}}) = 1/(3\log 2) = 0,48\ldots$(Haber 66). Since then, trying to reduce the gap between upper and lower bounds is still a challenge.

In the following, we consider the problem of finding best possible lower bounds within our new family of sequences $X_b^{\Sigma,C}$.

2. A lower bound for a family of $X_b^{\Sigma,C}$ seq.

Let $\tau \in \mathfrak{S}_b$ be the permutation defined by $\tau(k) = b - k - 1$ (all $k \in \mathbb{Z}_b$). For any subset $\mathcal{S}$ of integers and any $\sigma \in \mathfrak{S}_b$, define the sequence

$$\Sigma_{\mathcal{S}}^{\sigma} = (\sigma_r)_{r \geq 0} \text{ by } \sigma_r = \sigma \text{ if } r \in \mathcal{S} \text{ and } \sigma_r = \tau \circ \sigma =: \overline{\sigma} \text{ if } r \notin \mathcal{S}.$$

The permutation τ “swaps” the functions $\psi_b^{\sigma,+}$ and $\psi_b^{\sigma,-}$, that is $\psi_b^{\sigma,+} = \psi_b^{\tau\circ\sigma,-}$ and $\psi_b^{\sigma,-} = \psi_b^{\tau\circ\sigma,+}$. Thanks to that we can prove

Theorem 3. For any integer $b \geq 2$, let $\sigma \in \mathfrak{S}_b$ and let C be a strict upper triangular matrix with entries in $\mathbb{Z}_b$. Then, for any subset $\mathcal{S}$ of integers, we have

$$D^*(N, X_b^{\Sigma_{\mathcal{S}}^{\sigma},C}) \geq \frac{1}{2} D(N, S_b^{\sigma}) \quad \text{and hence} \quad s^*(X_b^{\Sigma_{\mathcal{S}}^{\sigma},C}) \geq \frac{\alpha_b^{\sigma}}{2 \log b},$$

where $\alpha_b^{\sigma} = \inf_{n \geq 1} \sup_{x \in [0,1]} \frac{1}{n} \sum_{j=1}^{n} \psi_b^{\sigma}\left(\frac{x}{b^j}\right)$.

Hint for Theorem 3: From Theorem 2, we obtain

$$D(N, X_b^{\Sigma_{\mathcal{S}}^{\sigma}, C}) = \sum_{j=1}^{\infty} \psi_b^{\sigma_{j-1}}\left(\frac{N}{b^j}\right) = \sum_{j=1}^{\infty} \psi_b^{\sigma}\left(\frac{N}{b^j}\right) = D(N, S_b^{\sigma}),$$

since $\sigma_{j-1} = \sigma$ or $\tau \circ \sigma$ so that $\psi_b^{\sigma_{j-1}} = \psi_b^{\sigma_{j-1},+} + \psi_b^{\sigma_{j-1},-} = \psi_b^{\sigma}$. Hence

$$D^*(N, S_b^{\Sigma_{\mathcal{S}}^{\sigma}}) \geq \frac{1}{2} D(N, S_b^{\Sigma_{\mathcal{S}}^{\sigma}}) = \frac{1}{2} D(N, S_b^{\sigma}).$$

Now, the last inequality follows since it is known (HF'81) that

$$\limsup_{N \to \infty} \frac{D(N, S_b^{\sigma})}{\log N} = \frac{\alpha_b^{\sigma}}{\log b}.$$

3. An optimized set for low star discrepancy

Let $\mathcal{A}$ be the subset $\mathcal{A} := \{0, 2, 3, 6, 7, 8, 12, 13, 14, 15, \ldots\}$, so that $\Sigma_{\mathcal{A}}^{\sigma} = (\sigma, \overline{\sigma}, \sigma, \sigma, \overline{\sigma}, \overline{\sigma}, \sigma, \sigma, \sigma, \overline{\sigma}, \overline{\sigma}, \overline{\sigma}, \ldots)$. Then (HF'81)

$$s^*(S_b^{\Sigma_{\mathcal{A}}^{\sigma}}) = \frac{\alpha_b^{\sigma,+} + \alpha_b^{\sigma,-}}{2 \log b} \text{ where}$$

$$\alpha_b^{\sigma,+} = \inf_{n \geq 1} \sup_{x \in [0,1]} \frac{1}{n} \sum_{j=1}^{n} \psi_b^{\sigma,+}\left(\frac{x}{b^j}\right) , \ \alpha_b^{\sigma,-} = \inf_{n \geq 1} \sup_{x \in [0,1]} \frac{1}{n} \sum_{j=1}^{n} \psi_b^{\sigma,-}\left(\frac{x}{b^j}\right).$$

This construction has given the lowest known star discrepancies, currently (Ostromoukhov'09): there exists a permutation $\sigma_0 \in \mathfrak{S}_{60}$ s.t.

$$s^*(S_{60}^{\Sigma_{\mathcal{A}}^{\sigma_0}}) = \frac{32209}{35400 \log 60} = 0.2222\ldots.$$

It is interesting to note that $\psi_{60}^{\sigma_0,-} = 0$, hence $D^*(S_{60}^{\Sigma_{\mathcal{A}}^{\sigma_0}}) = D(S_{60}^{\Sigma_{\mathcal{A}}^{\sigma_0}})$.

For reasonable small b, constants $\alpha_b^{\sigma,+}$ and $\alpha_b^{\sigma,-}$ are not difficult to compute and for identy, it is even possible to find them:

$$s^*(S_b^{\Sigma_{\mathcal{A}}^{\mathrm{id}}}) = \frac{\alpha_b^{I,+}}{2\log b} = \frac{b-1}{8\log b} \quad \text{if } b \text{ is odd, and}$$

$$s^*(S_b^{\Sigma_{\mathcal{A}}^{\mathrm{id}}}) = \frac{\alpha_b^{I,+}}{2\log b} = \frac{b^2}{8(b+1)\log b} \quad \text{if } b \text{ is even.}$$

4. Best possible lower bounds for $X_b^{\Sigma_{\mathcal{S}}^\sigma, C}$ seq.

Now, comparing the lower bound $s^*(X_b^{\Sigma_{\mathcal{S}}^\sigma, C}) \geq \dfrac{\alpha_b^\sigma}{2 \log b}$ for arbitrary sets $\mathcal{S}$ from Theorem 3 and the result with the set $\mathcal{A}$,

$$s^*(S_b^{\Sigma_{\mathcal{A}}^\sigma}) = \frac{\alpha_b^{\sigma,+} + \alpha_b^{\sigma,-}}{2 \log b},$$

we cannot infer any relation between them since in general we have

$$\alpha_b^\sigma \leq \alpha_b^{\sigma,+} + \alpha_b^{\sigma,-}.$$

But if we have either $\psi_b^{\sigma,+} = 0$ or $\psi_b^{\sigma,-} = 0$, in which case we get $\alpha_b^\sigma = \alpha_b^{\sigma,+} + \alpha_b^{\sigma,-}$, we obtain that $\alpha_b^\sigma/(2 \log b)$ is the best possible lower bound for the star discrepancy of sequences $X_b^{\Sigma_{\mathcal{S}}^\sigma, C}$:

Corollary 1 Let $\mathcal{C}_{SUT}$ be the set of all strict upper triangular matrices and let $\sigma \in \mathfrak{S}_b$ such that $D^*(S_b^\sigma) = D(S_b^\sigma)$. Then

$$\inf_{\substack{\Sigma \in \{\sigma, \tau\circ\sigma\}^{\mathbb{N}} \\ C \in \mathcal{C}_{SUT}}} s^*(X_b^{\Sigma,C}) = \frac{\alpha_b^\sigma}{2\log b}.$$

Hint: Theorem 3 implies that $\alpha_b^\sigma/(2\log b)$ is a lower bound and on the other hand, with the null matrix $C = 0$ and $\Sigma_{\mathcal{A}}^\sigma$, we have $X_b^{\Sigma_{\mathcal{A}}^\sigma, 0} = S_b^{\Sigma_{\mathcal{A}}^\sigma}$ so that

$$s^*(X_b^{\Sigma_{\mathcal{A}}^\sigma, 0}) = s^*(S_b^{\Sigma_{\mathcal{A}}^\sigma}) = \frac{\alpha_b^\sigma}{2\log b},$$

since in the present case we have $\alpha_b^\sigma = \alpha_b^{\sigma,+} + \alpha_b^{\sigma,-}$.

The case of identity in Corollary 1 is of special interest because α_b^{id} is explicitly known for any integer $b \geq 2$.

Corollary 2 With the notations of Corollary 1, we obtain

$$\inf_{b\geq 2} \inf_{\substack{\Sigma\in\{\mathrm{id},\tau\}^{\mathbb{N}} \\ C\in\mathcal{C}_{SUT}}} s^*(X_b^{\Sigma,C}) = s^*(S_3^{\Sigma_{\mathcal{A}}^{\mathrm{id}}}) = \frac{1}{4\log 3} = 0.2275\ldots.$$

This result can be seen as an analog (for van der Corput sequences and NUT $(0,1)$-sequences) of the result on $(n\alpha)$ sequences obtained by Dupain and Sós (1984):

$$\inf_{\alpha} s^*((n\alpha)) = s^*((n\sqrt{2})) = \frac{1}{4\log(\sqrt{2}+1)} = 0.2836\ldots.$$

5. Linearly digit scrambled NUT (0,1)-seq.

A *linear digit scrambling* (following Matoušek'98) is a permutation $\pi \in \mathfrak{S}_b$ of the form

$$\pi(k) = \gamma k + l \pmod b \text{ for all } k \in \mathbb{Z}_b, \text{ with } \gamma \neq 0, l \in \mathbb{Z}_b.$$

Let $\Pi = (\pi_r)_{r \geq 0} \in \mathfrak{S}_b^{\mathbb{N}}$ be a sequence of linear digit scramblings and let $\mathcal{C}^1_{NUT}$ be the set of NUT matrices C with all diagonal entries $c_r^r = 1$.

A linearly digit scrambled NUT digital (0,1)-sequence, denoted $Z_b^{\Pi,C}$, is defined by

$$Z_b^{\Pi,C}(N) = \sum_{r=0}^{\infty} \frac{\pi_r(x_{N,r})}{b^{r+1}} \quad \text{in which} \quad x_{N,r} = \sum_{k=r}^{\infty} c_r^k a_k(N) \pmod b.$$

Corollary 3 Let $Z_b^{\Pi,C}$ be a linearly digit scrambled NUT digital (0,1)-sequence associated with $C \in \mathcal{C}_{NUT}^1$ and $\Pi = (\pi_r)_{r\geq 0} \in \{\mathrm{id}, \tau\}^{\mathbb{N}}$. Then we have

$$\inf_{b\geq 2} \inf_{\substack{\Pi\in\{\mathrm{id},\tau\}^{\mathbb{N}} \\ C\in\mathcal{C}_{NUT}^1}} s^*(Z_b^{\Pi,C}) = \frac{1}{4\log 3} = 0.2275\ldots.$$

Hint: The permutation τ is a linear digit scrambling since

$$\tau(k) = (b-1)k + b - 1 \,(\mathrm{mod}\, b),$$

from which it is easy to prove that $Z_b^{\Pi,C} = X_b^{\Pi,C'}$ where $C' = \left((b-1)c_r^k\right)_{r\geq 0, k\geq r+1} \in \mathcal{C}_{SUT}$.

Remark: The only linear digit scramblings π verifying $D(S_b^\pi) = D^*(S_b^\pi)$ are permutations id and τ, as we checked recently.

Finally, we come back to the question that first motivated this study:

"Is it true that the constant $1/(6\log 2)$ is best possible for any digitally shifted NUT digital (0,1)-sequence in base 2, as it is the case for any digitally shifted van der Corput sequence?"

Since in base 2, the permutation τ is the nonzero shift and since the diagonal entries of C are all equal to 1, we can answer this question in the affirmative as a special case of Corollary 3:

Corollary 4 We have

$$\inf_{\substack{\Delta\in\mathbb{Z}_2^{\mathbb{N}}\\ C\in\mathcal{C}_{NUT}}} s^*(Z_2^{\Delta,C}) = \frac{1}{6\log 2} = 0.2404\ldots.$$

Thanks for your attention!