An extension of the digital method based on b-adic integers

Authors: Roswitha Hofer and Ísabel Pirsic
Speaker: Ísabel Pirsic
Affiliation: Johannes Kepler University Linz
Email: roswitha.hofer@jku.at, isabel.pirsic@jku.at
Funding: Austrian Science Fund, F5511-N26 (RH),
P27351-N26 (ÍP)

Discrepancy

- A 'measure for randomness' for point sets (as pertinent to specific applications)
- Distance from state of uniform distribution
- Worst case error of numerical integration of interval indicator functions
- Many versions: different choices of norms, measures, weights, anchoring, wrapping ...
- Here: star-discrepancy $D_N^*(P) = \sup_J |A_J/N - \lambda(J)|$
- Standard application: $|\int_I f - \frac{1}{N}\sum_P f| \le V(f) D_N^*(P)$
- Goal: low-discrepancy seq.s $N D_N^*(P) \approx O((\log N)^s)$
- Good choice: point sets/seq.s obtained by digital method $\rightsquigarrow$

Digital method (classical)

- Simple example of LDS : van der Corput sequence — reflection of digit expansion at decimal point: $2341 \mapsto 0.1432$
- Digital method : map digit vectors to vectors over finite ring, apply linear maps, map to $[0, 1)$ by fractional digit expansion

$$v_n = (\bar{n}_1, \bar{n}_2, \dots)^\top, \qquad \boxed{n = \sum_{i \geq 0} n_{i+1}\, b^i}$$

$$w_{n,i} = C_i \cdot v_n, \qquad \boxed{C_i \in \mathcal{M}at(R),\ {}_{i=1,\dots,s}}$$

$$= (\bar{x}_{n,i,1}, \bar{x}_{n,i,2}, \dots)^\top \mapsto \quad \boxed{x_{n,i} = \sum_{j>0} x_{n,i,j}\, b^{-j}}$$

  Vectors, matrices, may be finite or infinite, but n always has a finite expansion (and mat-vec prod.s exist). OTOH, $x_{n,i}$ need not, but is usually truncated to digit length of n.

- Discrepancy then related to the 'rank structure' of the matrices : $\boxed{T(m), t}$ -values defined by conditions of linear independence of <u>combinatorial subsets</u> of row vectors of C_i

The quality parameters $T(m), t$

- For integers m, t, $m \geq t \geq 0$ consider partitions $m - t = d_1 + \cdots + d_s$ into nonnegative integers and for each $i = 1, \ldots, s$ collect the initial d_i row vectors of C_i, truncated to the first m coordinates, in a new matrix. If for each partition the rank of this matrix is $m - t$ then $T(m) := m - t$ is called the **quality parameter at** m of a **digital** $(T(m), s)$**-sequence over** R.
- If $\lim_m (m - T(m)) = \infty$ then the sequence is UD.
- If $T(m) \leq t$ for all m then the sequence is an LDS with discrepancy bound

$$D_N^*(P) \in \mathcal{O}(b^t \frac{\log^s N}{N}).$$

- (Similar for a finite point set of size b^m
  $\rightsquigarrow$ **digital** (t, m, s)**-net over** R; $(s-1)$ in log-term)

b-adic integers $\mathbb{Z}_b$

- A subring of the ring $\mathbb{Q}_b$, b need not be prime
- Informally: Laurent series in b with $+, *, \ldots$ as in digit expansion vectors of $\mathbb{N}$. Then $\mathbb{Z}_b =$ set of power series in b.
- More formal: obtained by completion of $\mathbb{Q}$ with a (pseudo-)valuation ('absolute value'), inducing a non-archimedean metric. Then $\mathbb{Z}_b = \{a, |a|_b \leq 1\}$
- Examples: $|b^3 + b^5|_b = b^{-3}$, $|b^{-4} + b + 1|_b = b^4$, $|6|_{24} = |18|_{24} = 1/\sqrt[3]{24}$, $|12|_{24} = 1/\sqrt[3]{24^2}$.
- Usually: $\mathbb{Q}_p, p$ prime, generally $\mathbb{Q}_b \cong \mathbb{Q}_{p_1} \times \cdots \times \mathbb{Q}_{p_r}$, p_i the distinct prime divisors of b.
- $\mathbb{Z} \subsetneq \mathbb{Z}_b$ and $\mathbb{Z}_b$ is indeed a subring as above

Uniform distribution of sequences in $\mathbb{Z}, \mathbb{Z}_b$

- UD mod m: asymp. frequency $1/m$ for all residue classes
- UD mod $\mathbb{Z}$: UD mod m, for all $m > 1$
- UD mod $\mathbb{Z}_b$: k-digit truncations UD mod b^k, for all $k \geq 0$
- Trivial case: $(n)_{n \geq 0}$ is UD in $\mathbb{Z}_b$
- Some sequences UD in $\mathbb{Z}$ (thus also in $\mathbb{Z}_b$):
  - $(\lfloor \alpha n \rfloor)_{n \geq 0}$ for irrational α
  - $(\lfloor f(n) \rfloor)_{n \geq 0}$ for f polynomial where some coefficient apart from the constant is irrational.
  - $(\lfloor \alpha n^\sigma \rfloor)_{n \geq 0}$ for α arbitrary, σ positive, nonintegral.
- Also: $(an + c)_{n \geq 0}$ is UD in $\mathbb{Z}_b$ if $a \in \mathbb{Z}_b$ is a unit (constant term is relative prime to b), $c \in \mathbb{Z}_b$ arbitrary
- Not UD in $\mathbb{Z}_b$ (nor in $\mathbb{Z}$): e.g., $(n^2)_{n \geq 0}$

Extended Digital Method

- Choose some sequence $(s_n)_{n\geq 0}$ in $\mathbb{Z}_b$
  (i.e., its b-adic expansion) as input
  instead of $(n)_{n\geq 0}$ $\rightsquigarrow$ matrices need to have finite rows

Extended Digital Method

- Choose some sequence $(s_n)_{n\geq 0}$ in $\mathbb{Z}_b$
  (i.e., its b-adic expansion) as input
  instead of $(n)_{n\geq 0}$ $\rightsquigarrow$ matrices need to have finite rows
- Note 1: finite-row-matrices are important in base-mixing context

Extended Digital Method

- Choose some sequence $(s_n)_{n\geq 0}$ in $\mathbb{Z}_b$ (i.e., its b-adic expansion) as input instead of $(n)_{n\geq 0}$ $\rightsquigarrow$ matrices need to have finite rows
- Note 1: finite-row-matrices are important in base-mixing context
- Note 2: true generalization, since, e.g., identity matrix and $(\alpha n^2 + \beta)_{n\geq 0}$ give a sequence that can not be reproduced by the classical method (nonlinear, nonfinite input, b-adic shift).

Extended Digital Method

- Choose some sequence $(s_n)_{n\geq 0}$ in $\mathbb{Z}_b$ (i.e., its b-adic expansion) as input instead of $(n)_{n\geq 0}$ $\rightsquigarrow$ matrices need to have finite rows
- Note 1: finite-row-matrices are important in base-mixing context
- Note 2: true generalization, since, e.g., identity matrix and $(\alpha n^2 + \beta)_{n\geq 0}$ give a sequence that can not be reproduced by the classical method (nonlinear, nonfinite input, b-adic shift).
- **Theorem 1:** If (fin.row) matrices $C_i \in \mathcal{M}at_\infty(\mathbb{F}_q)$ classically generate a UD sequence and s_n is UD in $\mathbb{Z}_q$ then both generate a UD sequence in the extended algorithm.

Extended Digital Method

- Choose some sequence $(s_n)_{n\geq 0}$ in $\mathbb{Z}_b$ (i.e., its b-adic expansion) as input instead of $(n)_{n\geq 0}$ $\rightsquigarrow$ matrices need to have finite rows
- Note 1: finite-row-matrices are important in base-mixing context
- Note 2: true generalization, since, e.g., identity matrix and $(\alpha n^2 + \beta)_{n\geq 0}$ give a sequence that can not be reproduced by the classical method (nonlinear, nonfinite input, b-adic shift).
- **Theorem 1:** If (fin.row) matrices $C_i \in \mathcal{M}at_\infty(\mathbb{F}_q)$ classically generate a UD sequence and s_n is UD in $\mathbb{Z}_q$ then both generate a UD sequence in the extended algorithm.
- Converse does not hold: $(n^2)_{n\geq 0}$ not UD, but there is a simple matrix over $\mathbb{F}_2$ such that their combined sequence is UD

Extended Digital Method II

- **Theorem 2:** Let $C_1, \ldots, C_s$ be ∞-matrices over $\mathbb{F}_q$ with row length not exceeding their row index times s. If they generate a $(0, s)$-sequence then together with a sequence s_n in $\mathbb{Z}_q$ a UD sequence will be generated *if and only if* s_n is UD in $\mathbb{Z}_q$.

Extended Digital Method II

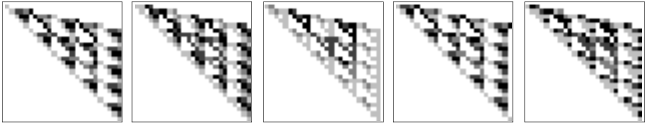
- **Theorem 2:** Let $C_1, \ldots, C_s$ be ∞-matrices over $\mathbb{F}_q$ with row length not exceeding their row index times s. If they generate a $(0, s)$-sequence then together with a sequence s_n in $\mathbb{Z}_q$ a UD sequence will be generated *if and only if* s_n is UD in $\mathbb{Z}_q$.
- Remark: The case $s = 1$ and $C_1 = Id$ was proven by Hellekallek and Niederreiter in a special case.

Extended Digital Method II

- **Theorem 2:** Let $C_1, \dots, C_s$ be ∞-matrices over $\mathbb{F}_q$ with row length not exceeding their row index times s. If they generate a $(0, s)$-sequence then together with a sequence s_n in $\mathbb{Z}_q$ a UD sequence will be generated *if and only if* s_n is UD in $\mathbb{Z}_q$.
- Remark: The case $s = 1$ and $C_1 = Id$ was proven by Hellekallek and Niederreiter in a special case.
- **Prop.2:** Discrepancy estimate for $(s_n)_{n \geq 0} = (n + \alpha)_{n \geq 0}$ and generators of a $(T(m), s)$-sequence.
- **Cor.2:** If additionally $T(m)$ is bounded then a low-discrepancy sequence is generated.
- **Cor.3:** If $T(m)$ is bounded and $gcd(v, q) = 1, \alpha$ arbitrary, then $s_n = \frac{1}{v} n + \alpha$ also generates a low-discrepancy sequence.

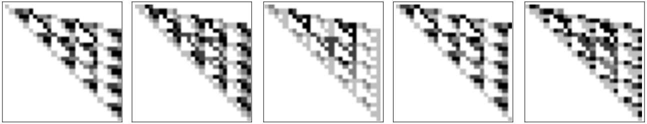
Numerical Experiments – Plots

- Using Stirling matrices over $\mathbb{F}_5$:



Numerical Experiments – Plots

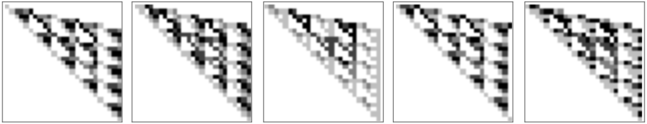
- Using Stirling matrices over $\mathbb{F}_5$:



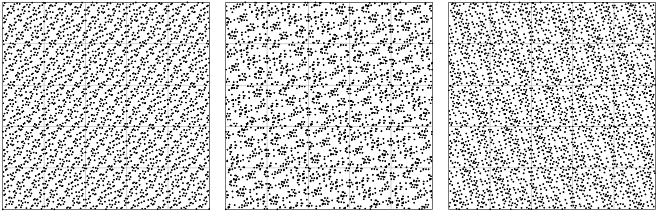
- And three different input sequences:
  - $s_n = n$
  - $s_n = \langle 1, -1, 2, -2, \dots \rangle$
  - $s_n = \frac{1}{2}n - \frac{1}{4}$

Numerical Experiments – Plots

- Using Stirling matrices over $\mathbb{F}_5$:



- And three different input sequences:
  - $s_n = n$
  - $s_n = \langle 1, -1, 2, -2, \dots \rangle$
  - $s_n = \frac{1}{2}n - \frac{1}{4}$
- ... produces these point sets (500 pts):



Numerical Experiments – 1d-discrepancy

- Using the identity matrix over $\mathbb{F}_2$

Numerical Experiments – 1d-discrepancy

- Using the identity matrix over $\mathbb{F}_2$
- And three different input sequences :

black $s_n = n$

gray $s_n = \langle 1, -1, 2, -2, \ldots \rangle$

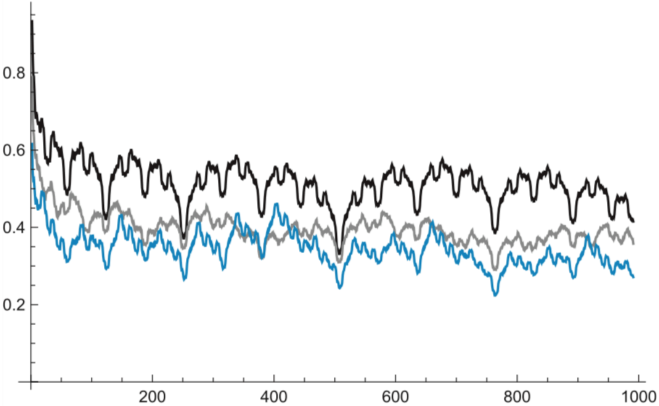
blue $s_n = n - 1/(2 + 2^{-1}) = n - 2/5$

Numerical Experiments – 1d-discrepancy

- Using the identity matrix over $\mathbb{F}_2$
- And three different input sequences :

black $s_n = n$
gray $s_n = \langle 1, -1, 2, -2, \dots \rangle$
blue $s_n = n - 1/(2 + 2^{-1}) = n - 2/5$

- ... gives the following discrepancies (divided by $\log N/N$):



Numerical Experiments – 2d-discrepancy

- Using the Stirling matrices over $\mathbb{F}_2$

Numerical Experiments – 2d-discrepancy

- Using the Stirling matrices over $\mathbb{F}_2$
- And three different input sequences :

black $s_n = n$

gray $s_n = -(n+1)$

blue $s_n = n - 1/(2 + 2^{-10}) = n - 1024/2049$

Numerical Experiments – 2d-discrepancy

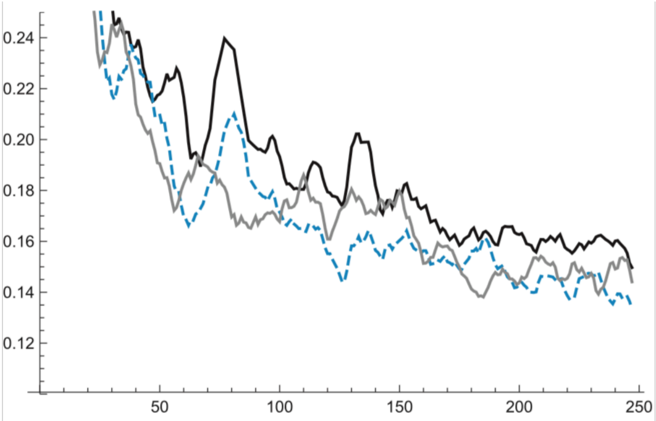
- Using the Stirling matrices over $\mathbb{F}_2$
- And three different input sequences :

black $s_n = n$

gray $s_n = -(n+1)$

blue $s_n = n - 1/(2 + 2^{-10}) = n - 1024/2049$

- … gives the following discrepancies (divided by $\log^2 N/N$):



Open to research (and to reflect)

- Determine const.s, e.g., for linear input seq.s more explicitly

Open to research (and to reflect)

- Determine const.s, e.g., for linear input seq.s more explicitly
- Composite b — Does anything unexpected happen ?

Open to research (and to reflect)

- Determine const.s, e.g., for linear input seq.s more explicitly
- Composite b — Does anything unexpected happen ?
- Many more input sequences, esp.polynomials;
  probably either not easy to investigate or not that good ...

Open to research (and to reflect)

- Determine const.s, e.g., for linear input seq.s more explicitly
- Composite b — Does anything unexpected happen ?
- Many more input sequences, esp.polynomials;
  probably either not easy to investigate or not that good ...
- What about sequences of algebraic integers
  (i.e., algebraic integers in some $\mathbb{Q}_p(\alpha)$)?

Open to research (and to reflect)

- Determine const.s, e.g., for linear input seq.s more explicitly
- Composite b — Does anything unexpected happen ?
- Many more input sequences, esp.polynomials;
  probably either not easy to investigate or not that good ...
- What about sequences of algebraic integers
  (i.e., algebraic integers in some $\mathbb{Q}_p(\alpha)$)?
- Conceptually interesting: UD in $\mathbb{Z}_b$, or analogously, in $\mathbb{F}_b[[x]]$, can be spread out to UD in $\mathbb{F}_b[[x]]^s$ by simple linear transformation — what kind of matrices suffice
  (do we really need the full (t,s)-property)?

Open to research (and to reflect)

- Determine const.s, e.g., for linear input seq.s more explicitly
- Composite b — Does anything unexpected happen ?
- Many more input sequences, esp.polynomials;
  probably either not easy to investigate or not that good ...
- What about sequences of algebraic integers
  (i.e., algebraic integers in some $\mathbb{Q}_p(\alpha)$)?
- Conceptually interesting: UD in $\mathbb{Z}_b$, or analogously, in $\mathbb{F}_b[[x]]$,
  can be spread out to UD in $\mathbb{F}_b[[x]]^s$ by simple linear
  transformation — what kind of matrices suffice
  (do we really need the full (t, s)-property)?
- Integrate a 'discrepancy in integers' into this frameweork

Open to research (and to reflect)

- Determine const.s, e.g., for linear input seq.s more explicitly
- Composite b — Does anything unexpected happen ?
- Many more input sequences, esp.polynomials;
  probably either not easy to investigate or not that good ...
- What about sequences of algebraic integers
  (i.e., algebraic integers in some $\mathbb{Q}_p(\alpha)$)?
- Conceptually interesting: UD in $\mathbb{Z}_b$, or analogously, in $\mathbb{F}_b[[x]]$, can be spread out to UD in $\mathbb{F}_b[[x]]^s$ by simple linear transformation — what kind of matrices suffice
  (do we really need the full (t, s)-property)?
- Integrate a 'discrepancy in integers' into this frameweork
- Silly questions : — Where does the powerful randomness of multivariate digital sequences 'come from'? $\mathbb{Z}_b$? $\mathbb{F}_b^{\mathbb{N}}$? Or which one rather, of the maps

$$v_n : \mathbb{Z}_b \mapsto \mathbb{F}_b^{\mathbb{N}}, \quad (C_i)_i : \mathbb{F}_b[[x]] \mapsto \mathbb{F}_b[[x]]^s?$$

The End.

Thank you

for your kind attention !