Low-discrepancy point sets and sequences

1. Extending the van der Corput sequence to $s > 1$
   - Halton sequence
   - Digital Sequences (ex: Sobol', Faure)
2. Lattices

Extending the van der Corput sequence to $s > 1$

How do we do this? First approach:

- use a different base for each dimension (Halton sequence, 1960).
- That is, let S_b denote the van der Corput sequence in base b, and $S_b(n)$ be the nth term of this sequence.
- The Halton sequence in s dimensions is given by $(S_{b_1}, \ldots, S_{b_s})$ where the b_j's are pairwise co-primes.
- Typically, take b_j to be the jth prime number.

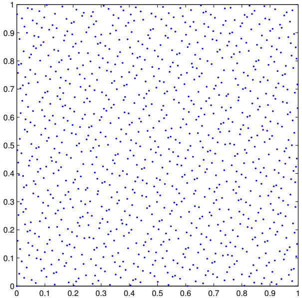
Advantages: simple to understand and implement.

Disadvantages: doesn't work so well in medium to high dimensions (say above 40 or 50)

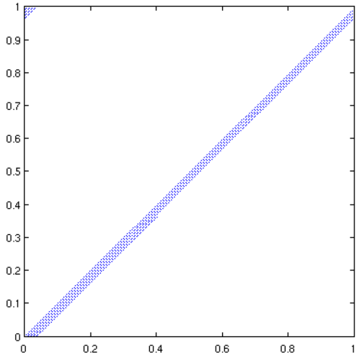
Halton sequence

$$\mathbf{u}_1 = (0, 0, 0, \ldots) \qquad \mathbf{u}_2 = (1/2, 1/3, 1/5, \ldots)$$
$$\mathbf{u}_3 = (1/4, 2/3, 2/5, \ldots) \qquad \mathbf{u}_4 = (3/4, 1/9, 3/5, \ldots)$$
$$\mathbf{u}_5 = (1/8, 4/9, 4/5, \ldots)$$

First two dimensions:



1000 first points of the Halton sequence defined with p_{49} and p_{50} (49th and 50th prime numbers ($p_{49} = 227$ and $p_{50} = 229$))



Second approach to extend VDC to $s > 1$

- If we want to use the same base b in each dimension, can "individualize" the different coordinates by applying a **linear transformation** to the digits in the base b expansion of i.
- First construction based on this idea is the Sobol' sequence (1967).
- More general definition is that of **digital sequences**.

Digital sequence in base b

(Not explained in their full generality here.)

- Choose s **generating matrices** $C_1, \ldots, C_s$ in base b
- Apply C_j to the digits $a_{i,0}, a_{i,1}, \ldots$ coming from the expansion of i in base b to construct jth coordinate. More precisely the jth coordinate $u_{i,j}$ of the ith point $\mathbf{u}_i$ of the sequence is obtained by computing

$$\mathbf{C}_j \begin{pmatrix} a_{i,0} \\ a_{i,1} \\ \vdots \end{pmatrix} = \begin{pmatrix} y_{ij1} \\ y_{ij2} \\ \vdots \\ y_{ijk} \\ \vdots \end{pmatrix}$$

and let $u_{ij} = y_{ij1} b^{-1} + y_{ij2} b^{-2} + \ldots + y_{ijk} b^{-k} + \ldots, \qquad j = 1, \ldots, s.$

Digital net

- Refers to finite point set P_n obtained from the first n points of a digital sequence.
- Can be obtained using same approach but, say for $n = b^m$, only need m columns for generating matrices.

Sobol' sequence

- The jth generating matrix C_j is constructed **column by column**, using a recurrence in base 2 to obtain lth column from preceding d_j columns, where d_j is the **order** of the recurrence. Need for each j:
  1. primitive polynomial in base 2 (let its degree be d_j) whose coefficients define the recurrence
  2. "direction numbers" that initialize the first d_j columns
- Direction numbers up to dimension $s = 40$ given by Sobol' initially, who choose them carefully (realized their importance).
- Other people have proposed direction numbers for larger dimensions since then.
- Implementations in Matlab, R (qrng package), Python (QMCPy software by Hickernell et al.)
- Because of its binary nature, Sobol' sequence can be generated very quickly (faster than most PRNGs).

Faure sequence (1982)

- Must choose base $b \geqslant s$.
- Take C_j to be the $(j-1)$th power of the Pascal matrix P in base b.

$$P = \begin{pmatrix} 1 & \binom{2}{1} \bmod b & \binom{3}{1} \bmod b & \dots \\ 0 & 1 & \binom{2}{2} \bmod b & \binom{3}{2} \bmod b \\ \vdots & \dots & & \end{pmatrix}$$

- Example with $b = 3$ and $s = 3$: say we want u_{11}:

$11 = 2 \times 3^0 + 0 \times 3^1 + 1 \times 3^2$ and $u_{11,1} = 2/3 + 1/27 = 19/27$ since

$$\underbrace{\begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}}_{C_1} \begin{pmatrix} 2 \\ 0 \\ 1 \end{pmatrix} = \begin{pmatrix} 2 \\ 0 \\ 1 \end{pmatrix}$$

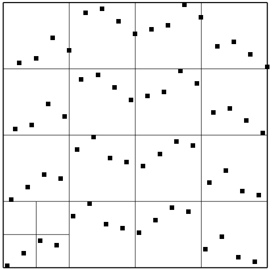
Faure sequence: why choose the Pascal matrices?

- Because the obtained sequence can then be shown to be a $(0, s)$-sequence... i.e., its t-value is 0. What does this mean?
- t-value of a sequence measures its uniformity; smallest t is, smallest is the discrepancy. Has to do with the **equidistribution** of the sequence.
- In his 1967 paper, Sobol' defined this parameter t for his construction.

Equidistribution

First define concept of *resolution* ℓ_s in base b as

$$\ell_s \quad = \quad \max_{l}\{\text{ partition of } [0,1)^s \text{ into } b^{sl} \text{ cubic boxes has } n/b^{sl} \text{ points in each box}\}$$

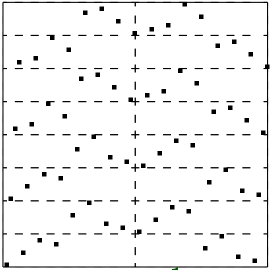


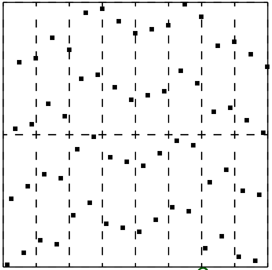
base 2

$n = 64$

Here, $\ell_2 = 2$. Maximal resolution would be 3 (1 pt per box in 8×8 grid).
Both $P_n(\{1\}) = \{u_{i,1}, 1 \leqslant i \leqslant n\}$ and $P_n(\{2\}) = \{u_{i,2}, 1 \leqslant i \leqslant n\}$ have $\ell_1 = 6$.

t-value: not restricted to cubic boxes





$(q_1, \ldots, q_s)$-*equidistribution*: must have n/b^q points in each b-ary box

$$\prod_{j=1}^{s} \left[\frac{l}{b^{q_j}}, \frac{l+1}{b^{q_j}} \right), \qquad 0 \leqslant l < b^{q_j}, \text{ where } q = q_1 + \ldots + q_s.$$

Then $t = \log_b n - \max\{k\colon (q_1, \ldots, q_s)\text{-equid. if } q_1 + \ldots + q_s \leqslant k\}$.

ex: Above, $t = \log_2 64 - 4 = 2$ $\qquad$ ($q_1 = q_2 = 2$ also works)

Back to Faure sequences

The first $n = b^m$ points of a Faure sequence in base $b \geqslant s$ always have $t = 0$

$\Rightarrow (0, m, s)$–**net in base** b

Back to: Low-discrepancy point sets and sequences

1. Extending the van der Corput sequence to $s > 1$
   - Halton sequence
   - Digital Sequences (ex: Sobol', Faure)
2. Lattices
   - Simplest case is a **Korobov lattice**: we'll focus on this first.

Korobov lattices (1959)

- Very simple construction; easy to implement from scratch; quick.
- To generate n points in $[0,1)^s$, choose an integer $a \in \{1, \ldots, n-1\}$ such that $\gcd(a, n) = 1$ and take

$$P_n = \left\{ \frac{i}{n} \, (1, a, a^2, \ldots, a^{s-1} \bmod n) \bmod 1, i = 0, \ldots, n-1 \right\}.$$

- ex.: $n = 16, a = 5 \Rightarrow P_n = \{(0,0), (\frac{1}{16}, \frac{5}{16}), (\frac{2}{16}, \frac{10}{16}), \ldots, (\frac{15}{16}, \frac{11}{16})\}$
- Tables of "good" a are available (example: L'Ecuyer and Lemieux, Management Science, 2000 (Variance Reduction via Lattice Rules))
- The condition $\gcd(a, n) = 1$ guarantees each one-dimensional projection has n distinct points, i.e., $P_n(\{j\} = \{u_{ij}, i = 0, \ldots, n-1\} = \{0, 1/n, 2/n, \ldots, (n-1)/n\}$.
- Can also be made extensible, i.e., no need to specify n ahead of time.

Pseudocode to generate Korobov lattice points

```
InitKorobov(a, n, s, z)
    z(1) ← 1
    for j = 2 to s
        z(j) ← a × z(j − 1) mod n
//
NextKorobov(n, z, u) // u is the previous point
    return ((u + z/n) mod 1)
//
GenKorobov(a, n, s)
    u ← 0
    InitKorobov(a, n, s, z)
    for i = 1 to n − 1
        u ← NextKorobov(n, z, u)
```

Connection between Korobov lattice and LCG

- A Korobov lattice P_n in dimension s with n points and with generator a corresponds to the set Ψ_s obtained from an LCG based on modulus n and multiplier a.
- Gives an alternative way of generating points from P_n when a and n are such that the LCG has a **maximal period of $n-1$**: run the LCG from x_0 to $x_{n-2+(s-1)}$; form successive (overlapping) s-dimensional points
- $\mathbf{u}_1 = (0, \ldots, 0)$, $\mathbf{u}_2 = (x_0, x_1, \ldots, x_{s-1})$, $\mathbf{u}_3 = (x_1, \ldots, x_s)$,. . . , $\mathbf{u}_n = (x_{n-2}, \ldots, x_{n-2+s-1})$
- Especially useful for problems where **we don't know the dimension s *a priori*** (e.g., bank example)

Rank-1 lattices

- Korobov lattices are a special case of **rank-1 lattices**
- A rank-1 lattice is defined by a **generating vector** $\mathbf{z} = (z_1, \ldots, z_s)$
- Korobov lattice takes $z_j = a^{j-1} \bmod n, j = 1 \ldots, s$
- Typically takes z_j so that $\gcd(z_j, n) = 1$: this way each one-dimensional projection of the lattice
$$P_n(\{j\}) = \left\{ \frac{i}{n} z_j \bmod 1, i = 0, \ldots, n-1 \right\}$$
yields the n distinct points $\{0, 1/n, \ldots, (n-1)/n\}$.
- Sloan and collaborators have developed “component-by-component” searches to find the z_j’s successively so as to minimize, at each step j, the worst-case integration error over a class of (smooth) functions in j dimensions.
- Tables of good generating vectors exist (see Frances Kuo’s website).

Polynomial lattices

- Has connections with both lattices and digital nets
- Connection with lattices: replace

$$\mathbb{Z} \to \mathbb{F}_b[z] \qquad \mathbb{Z}_n \to \underbrace{\mathbb{F}_b[z]/((p(z))}_{\text{ring of polyn. mod } p(z)} \qquad \mathbb{Q} \to \underbrace{\mathbb{F}_b((z^{-1}))}_{\text{field of formal Laurent series over } \mathbb{F}_b}$$

then replace

$$P_n = \left\{ \frac{i}{n}(z_1, \ldots, z_s), i \in \mathbb{Z}_n \right\}$$

with

$$P_n(z) = \left\{ \frac{q(z)}{p(z)}(g_1(z), \ldots, g_s(z)), q(z) \in \mathbb{F}_b[z]/((p(z)) \right\}$$

To get P_n from $P_n(z)$, apply $\psi : \frac{r(z)}{p(z)} = a_1 z^{-1} + a_2 z^{-2} + \ldots \to a_1 b^{-1} + a_2 b^{-2} + \ldots$

Polynomial lattices (continued)

- Correspond to digital nets where C_j is of the form

$$C_j = \begin{pmatrix} a_{j,1} & a_{j,2} & \cdots & a_{j,m} \\ a_{j,2} & a_{j,3} & \iddots & a_{j,m+1} \\ \iddots & \iddots & \iddots & \vdots \\ a_{j,m} & a_{j,m+1} & \cdots & \end{pmatrix}$$

- Connections with lattices **and** digital nets can both be used to understand properties of this construction
- Also connected to Tausworthe-type (combined or not) generators in the same way Korobov lattices are connected to LCGs