Recent Results for the Discrepancy of Polynomial Lattice Point Sets

Friedrich Pillichshammer¹

Linz/Austria

Joint work with Josef Dick, Aicke Hinrichs, Peter Kritzer, Gunther Leobacher and Wolfgang Ch. Schmid

¹Supported by the Austrian Science Foundation (FWF), Project S9609.

We want to approximate an integral

$$I_{s}(f) = \int_{[0,1]^{s}} f(\mathbf{x}) \, \mathrm{d}\mathbf{x}$$

using a QMC rule

$$Q_{N,s}(f) = \frac{1}{N} \sum_{n=0}^{N-1} f(\mathbf{x}_n)$$

where $x_0, ..., x_{N-1} \in [0, 1)^s$.

We want to approximate an integral

$$I_{\mathfrak{s}}(f) = \int_{[0,1]^{\mathfrak{s}}} f(\mathbf{x}) \, \mathrm{d}\mathbf{x}$$

using a QMC rule

$$Q_{N,s}(f) = \frac{1}{N} \sum_{n=0}^{N-1} f(\mathbf{x}_n)$$

where $x_0, ..., x_{N-1} \in [0, 1)^s$.

Point sets with good distribution properties yield a small error.

Koksma-Hlawka inequality

$$|I_s(f) - Q_{N,s}(f)| \leq V(f) D_N^*(\mathcal{P}),$$

where

- V(f) is a measure for the variation of f;
- D_N^* is the star discrepancy of the nodes $\mathcal{P} = \{\mathbf{x}_0, \dots, \mathbf{x}_{N-1}\}$.

Koksma-Hlawka inequality

$$|I_s(f) - Q_{N,s}(f)| \leq V(f)D_N^*(\mathcal{P}),$$

where

- V(f) is a measure for the variation of f;
- D_N^* is the star discrepancy of the nodes $\mathcal{P} = \{\mathbf{x}_0, \dots, \mathbf{x}_{N-1}\}$.

For $\mathbf{z} \in [0, 1]^s$ let

$$\Delta_{\mathcal{P}}(\mathbf{z}) := \frac{|\{\mathbf{0} \le n < N : \mathbf{x}_n \in [\mathbf{0}, \mathbf{z})\}|}{N} - \lambda_s([\mathbf{0}, \mathbf{z})).$$

Koksma-Hlawka inequality

$$|I_s(f) - Q_{N,s}(f)| \leq V(f)D_N^*(\mathcal{P}),$$

where

- V(f) is a measure for the variation of f;
- D_N^* is the star discrepancy of the nodes $\mathcal{P} = \{\mathbf{x}_0, \dots, \mathbf{x}_{N-1}\}$.

For $\mathbf{z} \in [0, 1]^s$ let

$$\Delta_{\mathcal{P}}(\mathbf{z}) := \frac{|\{\mathbf{0} \le n < N : \mathbf{x}_n \in [\mathbf{0}, \mathbf{z})\}|}{N} - \lambda_s([\mathbf{0}, \mathbf{z})).$$

Definition (star discrepancy)

$$D^*_N(\mathcal{P}) := \sup_{\mathsf{z} \in [0,1]^s} |\Delta_\mathcal{P}(\mathsf{z})|$$

Lower bound on D_N^* (Roth 1954; Schmidt 1972; Bilyk, Lacey, Vagharshakyan 2008)

For $s \in \mathbb{N}$ there exists $c_s > 0$ and $0 < \delta_s < \frac{1}{2}$ such that for all $\mathcal{P} \subseteq [0,1)^s$

$$D_N^*(\mathcal{P}) \ge c_s \frac{(\log N)^{\kappa_s}}{N}$$
 where $N = |\mathcal{P}|$

and where $\kappa_1 = 0$, $\kappa_2 = 1$ and $\kappa_s \geq \frac{s-1}{2} + \delta_s$ for s > 2.

Lower bound on D_N^* (Roth 1954; Schmidt 1972; Bilyk, Lacey, Vagharshakyan 2008)

For $s \in \mathbb{N}$ there exists $c_s > 0$ and $0 < \delta_s < \frac{1}{2}$ such that for all $\mathcal{P} \subseteq [0,1)^s$

$$D_N^*(\mathcal{P}) \geq c_s rac{(\log N)^{\kappa_s}}{N}$$
 where $N = |\mathcal{P}|$

and where $\kappa_1 = 0$, $\kappa_2 = 1$ and $\kappa_s \geq \frac{s-1}{2} + \delta_s$ for s > 2.

Point sets with $D_N^*(\mathcal{P}) \ll_s \frac{(\log N)^{\beta_s}}{N}$ are called **low discrepancy point sets**.

Lower bound on D_N^* (Roth 1954; Schmidt 1972; Bilyk, Lacey, Vagharshakyan 2008)

For $s \in \mathbb{N}$ there exists $c_s > 0$ and $0 < \delta_s < \frac{1}{2}$ such that for all $\mathcal{P} \subseteq [0,1)^s$

$$D^*_N(\mathcal{P}) \geq c_s rac{(\log N)^{\kappa_s}}{N}$$
 where $N = |\mathcal{P}|$

and where $\kappa_1 = 0$, $\kappa_2 = 1$ and $\kappa_s \ge \frac{s-1}{2} + \delta_s$ for s > 2.

Point sets with $D_N^*(\mathcal{P}) \ll_s \frac{(\log N)^{\beta_s}}{N}$ are called **low discrepancy point sets**.

- van der Corput-Halton sequences and Hammersley point sets;
- good lattice point sets (Korobov and Hlawka);
- (*t*, *m*, *s*)-nets, polynomial lattice point sets (Niederreiter).

Definition (Niederreiter 1987)

A point set \mathcal{P} consisting of b^m points in $[0,1)^s$ is called (t, m, s)-net in base b if every interval of the form

$$\prod_{i=1}^{s}\left[rac{a_{i}}{b^{d_{i}}},rac{a_{i}+1}{b^{d_{i}}}
ight)\subseteq [0,1)^{s}$$

of volume b^{t-m} contains exactly b^t points of \mathcal{P} .

Definition (Niederreiter 1987)

A point set \mathcal{P} consisting of b^m points in $[0,1)^s$ is called (t, m, s)-net in base b if every interval of the form

$$\prod_{i=1}^{s}\left[rac{a_{i}}{b^{d_{i}}},rac{a_{i}+1}{b^{d_{i}}}
ight)\subseteq [0,1)^{s}$$

of volume b^{t-m} contains exactly b^t points of \mathcal{P} .

• Any \mathcal{P} consisting of b^m points in $[0,1)^s$ is a (m,m,s)-net in base b;

Definition (Niederreiter 1987)

A point set \mathcal{P} consisting of b^m points in $[0,1)^s$ is called (t, m, s)-net in base b if every interval of the form

$$\prod_{i=1}^{s}\left[rac{a_{i}}{b^{d_{i}}},rac{a_{i}+1}{b^{d_{i}}}
ight)\subseteq [0,1)^{s}$$

of volume b^{t-m} contains exactly b^t points of \mathcal{P} .

- Any \mathcal{P} consisting of b^m points in $[0,1)^s$ is a (m,m,s)-net in base b;
- small quality parameter 0 ≤ t ≤ m implies good distribution properties;

Definition (Niederreiter 1987)

A point set \mathcal{P} consisting of b^m points in $[0,1)^s$ is called (t, m, s)-net in base b if every interval of the form

$$\prod_{i=1}^{s}\left[rac{a_{i}}{b^{d_{i}}},rac{a_{i}+1}{b^{d_{i}}}
ight)\subseteq [0,1)^{s}$$

of volume b^{t-m} contains exactly b^t points of \mathcal{P} .

- Any \mathcal{P} consisting of b^m points in $[0,1)^s$ is a (m,m,s)-net in base b;
- small quality parameter 0 ≤ t ≤ m implies good distribution properties;
- Niederreiter: if \mathcal{P} is a (t, m, s)-net in base b, then

$$D_{b^m}^*(\mathcal{P}) \ll_{s,b} b^t \frac{m^{s-1}}{b^m} \quad \left(\ll_{s,b} b^t \frac{(\log N)^{s-1}}{N} \right).$$

Let $b \in \mathbb{P}$ and let \mathbb{Z}_b be the finite field with b elements.

Let $b \in \mathbb{P}$ and let \mathbb{Z}_b be the finite field with b elements.

• choose $C_1, \ldots, C_s \in \mathbb{Z}_b^{m \times m}$;

Let $b \in \mathbb{P}$ and let \mathbb{Z}_b be the finite field with b elements.

- choose $C_1, \ldots, C_s \in \mathbb{Z}_b^{m \times m}$;
- for $n \in \{0, ..., b^m 1\}$ and $i \in \{1, ..., s\}$:

Let $b \in \mathbb{P}$ and let \mathbb{Z}_b be the finite field with b elements.

- choose $C_1, \ldots, C_s \in \mathbb{Z}_b^{m \times m}$;
- for $n \in \{0, ..., b^m 1\}$ and $i \in \{1, ..., s\}$:

 $n\mapsto \vec{n}$

Let $b \in \mathbb{P}$ and let \mathbb{Z}_b be the finite field with b elements.

- choose $C_1, \ldots, C_s \in \mathbb{Z}_b^{m \times m}$;
- for $n \in \{0, ..., b^m 1\}$ and $i \in \{1, ..., s\}$:

 $n \mapsto \vec{n} \mapsto \vec{y}_i := C_i \vec{n}$

Let $b \in \mathbb{P}$ and let \mathbb{Z}_b be the finite field with b elements.

- choose $C_1, \ldots, C_s \in \mathbb{Z}_b^{m \times m}$;
- for $n \in \{0, ..., b^m 1\}$ and $i \in \{1, ..., s\}$:

$$n \mapsto \vec{n} \mapsto \vec{y}_i := C_i \vec{n} \mapsto x_n^{(i)} := \frac{y_{i,1}}{b} + \dots + \frac{y_{i,m}}{b^m}$$

Let $b \in \mathbb{P}$ and let \mathbb{Z}_b be the finite field with b elements.

- choose $C_1, \ldots, C_s \in \mathbb{Z}_b^{m \times m}$;
- for $n \in \{0, ..., b^m 1\}$ and $i \in \{1, ..., s\}$:

$$n \mapsto \vec{n} \mapsto \vec{y}_i := C_i \vec{n} \mapsto x_n^{(i)} := \frac{y_{i,1}}{b} + \dots + \frac{y_{i,m}}{b^m}$$

•
$$\mathbf{x}_n = (x_n^{(1)}, \dots, x_n^{(s)}).$$

Let $b \in \mathbb{P}$ and let \mathbb{Z}_b be the finite field with b elements.

- choose $C_1, \ldots, C_s \in \mathbb{Z}_b^{m \times m}$;
- for $n \in \{0, ..., b^m 1\}$ and $i \in \{1, ..., s\}$:

$$n \mapsto \vec{n} \mapsto \vec{y}_i := C_i \vec{n} \mapsto x_n^{(i)} := \frac{y_{i,1}}{b} + \dots + \frac{y_{i,m}}{b^m}$$

•
$$\mathbf{x}_n = (x_n^{(1)}, \dots, x_n^{(s)}).$$

 $\mathcal{P} = \{\mathbf{x}_0, \dots, \mathbf{x}_{b^m-1}\}$ is a (t, m, s)-net in base b for some $0 \le t \le m$.

Let $b \in \mathbb{P}$ and let \mathbb{Z}_b be the finite field with b elements.

- choose $C_1, \ldots, C_s \in \mathbb{Z}_b^{m \times m}$;
- for $n \in \{0, ..., b^m 1\}$ and $i \in \{1, ..., s\}$:

$$n \mapsto \vec{n} \mapsto \vec{y}_i := C_i \vec{n} \mapsto x_n^{(i)} := \frac{y_{i,1}}{b} + \dots + \frac{y_{i,m}}{b^m}$$

•
$$\mathbf{x}_n = (x_n^{(1)}, \dots, x_n^{(s)}).$$

 $\mathcal{P} = \{\mathbf{x}_0, \dots, \mathbf{x}_{b^m-1}\}$ is a (t, m, s)-net in base b for some $0 \le t \le m$.

Definition

 \mathcal{P} is called a **digital** (t, m, s)-net over \mathbb{Z}_b .

Let $b \in \mathbb{P}$ and let \mathbb{Z}_b be the finite field with b elements.

- choose $C_1, \ldots, C_s \in \mathbb{Z}_b^{m \times m}$;
- for $n \in \{0, ..., b^m 1\}$ and $i \in \{1, ..., s\}$:

$$n \mapsto \vec{n} \mapsto \vec{y}_i := C_i \vec{n} \mapsto x_n^{(i)} := \frac{y_{i,1}}{b} + \dots + \frac{y_{i,m}}{b^m}$$

•
$$\mathbf{x}_n = (x_n^{(1)}, \dots, x_n^{(s)}).$$

 $\mathcal{P} = \{\mathbf{x}_0, \dots, \mathbf{x}_{b^m-1}\}$ is a (t, m, s)-net in base b for some $0 \le t \le m$.

Definition

 \mathcal{P} is called a **digital** (t, m, s)-net over \mathbb{Z}_b .

t depends only on the generating matrices C_1, \ldots, C_s .

Let b = 2, s = 2 and m = 4.

Let b = 2, s = 2 and m = 4. Choose the matrices

$$C_1 = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} \text{ and } C_2 = \begin{pmatrix} 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \end{pmatrix}.$$

We construct x_5 .

We construct x_5 . In base 2 we have

$$5 = 1 + 0 \cdot 2^1 + 1 \cdot 2^2 + 0 \cdot 2^3.$$

We construct x_5 . In base 2 we have

$$5 = 1 + 0 \cdot 2^1 + 1 \cdot 2^2 + 0 \cdot 2^3.$$

Now

$$C_1 \begin{pmatrix} 1\\0\\1\\0 \end{pmatrix} = \begin{pmatrix} 1\\0\\1\\0 \end{pmatrix} \text{ and } C_2 \begin{pmatrix} 1\\0\\1\\0 \end{pmatrix} = \begin{pmatrix} 0\\1\\0\\1 \end{pmatrix}.$$

We construct x_5 . In base 2 we have

$$5 = 1 + 0 \cdot 2^1 + 1 \cdot 2^2 + 0 \cdot 2^3.$$

Now

$$C_{1}\begin{pmatrix}1\\0\\1\\0\end{pmatrix} = \begin{pmatrix}1\\0\\1\\0\end{pmatrix} \text{ and } C_{2}\begin{pmatrix}1\\0\\1\\0\end{pmatrix} = \begin{pmatrix}0\\1\\0\\1\end{pmatrix}$$
$$x_{5}^{(1)} = \frac{1}{2} + \frac{1}{2^{3}} = \frac{5}{8} \text{ and } x_{5}^{(2)} = \frac{1}{2^{2}} + \frac{1}{2^{4}} = \frac{5}{16}$$

Hence

.

We construct x_5 . In base 2 we have

$$5 = 1 + 0 \cdot 2^1 + 1 \cdot 2^2 + 0 \cdot 2^3.$$

Now

Hence

and

$$C_{1}\begin{pmatrix}1\\0\\1\\0\end{pmatrix} = \begin{pmatrix}1\\0\\1\\0\end{pmatrix} \text{ and } C_{2}\begin{pmatrix}1\\0\\1\\0\end{pmatrix} = \begin{pmatrix}0\\1\\0\\1\end{pmatrix}$$
$$x_{5}^{(1)} = \frac{1}{2} + \frac{1}{2^{3}} = \frac{5}{8} \text{ and } x_{5}^{(2)} = \frac{1}{2^{2}} + \frac{1}{2^{4}} = \frac{5}{16}$$
$$\mathbf{x}_{5} = \begin{pmatrix}\frac{5}{8}, \frac{5}{16}\end{pmatrix}.$$

.



Figure: (0, 4, 2)-net over \mathbb{Z}_2 generated from C_1 and C_2 .



Figure: (0, 4, 2)-net over \mathbb{Z}_2 generated from C_1 and C_2 .



Figure: (0, 4, 2)-net over \mathbb{Z}_2 generated from C_1 and C_2 .



Figure: (0, 4, 2)-net over \mathbb{Z}_2 generated from C_1 and C_2 .



Figure: (0, 4, 2)-net over \mathbb{Z}_2 generated from C_1 and C_2 .



Figure: (0, 4, 2)-net over \mathbb{Z}_2 generated from C_1 and C_2 .
Lattice point sets

Lattice point set (Korobov, Hlawka) For $N \ge 2$ and $\mathbf{g} \in \mathbb{Z}^s$ let $\mathbf{x}_n = \left\{\frac{n}{N}\mathbf{g}\right\}$ for $0 \le n < N$.

Lattice point sets

Lattice point set (Korobov, Hlawka) For $N \ge 2$ and $\mathbf{g} \in \mathbb{Z}^s$ let

$$\mathbf{x}_n = \left\{ \frac{n}{N} \mathbf{g}
ight\}$$
 for $0 \le n < N$.

Polynomial lattice point sets are in their over all structure very similar to (classical) lattice point sets.

lattice point set	polynomial lattice point set
based on	based on
number theoretic concepts	algebraic methods
	(polynomial arithmetic)

Let $\mathbb{Z}_b((x^{-1}))$ be the field of **formal Laurent series** over \mathbb{Z}_b (*b* prime). Its elements are of the form

$$L = \sum_{\ell=w}^{\infty} t_{\ell} x^{-\ell}$$
 where $w \in \mathbb{Z}$ and $t_{\ell} \in \mathbb{Z}_b$.

Let $\mathbb{Z}_b((x^{-1}))$ be the field of **formal Laurent series** over \mathbb{Z}_b (*b* prime). Its elements are of the form

$$L = \sum_{\ell=w}^{\infty} t_{\ell} x^{-\ell}$$
 where $w \in \mathbb{Z}$ and $t_{\ell} \in \mathbb{Z}_b$.

For $m \in \mathbb{N}$ let

$$\nu_m:\mathbb{Z}_b((x^{-1}))\to [0,1)$$

$$\nu_m\left(\sum_{\ell=w}^{\infty} t_\ell x^{-\ell}\right) = \sum_{\ell=\max(1,w)}^m t_\ell b^{-\ell}.$$

Let $\mathbb{Z}_b((x^{-1}))$ be the field of **formal Laurent series** over \mathbb{Z}_b (*b* prime). Its elements are of the form

$$L = \sum_{\ell=w}^{\infty} t_{\ell} x^{-\ell}$$
 where $w \in \mathbb{Z}$ and $t_{\ell} \in \mathbb{Z}_b$.

For $m \in \mathbb{N}$ let

$$\nu_m:\mathbb{Z}_b((x^{-1}))\to [0,1)$$

$$\nu_m\left(\sum_{\ell=w}^{\infty}t_\ell x^{-\ell}\right)=\sum_{\ell=\max(1,w)}^m t_\ell b^{-\ell}.$$

Let $G_{b,m} := \{h \in \mathbb{Z}_b[x] : \deg(h) < m\}$. We have $|G_{b,m}| = b^m$.

Definition (Niederreiter 1992)

For $s, m \in \mathbb{N}$, choose $p \in \mathbb{Z}_b[x]$ with deg(p) = m, and $\mathbf{q} \in \mathbb{Z}_b[x]^s$. The point set consisting of the b^m points

$$\mathbf{x}_h =
u_m \left(rac{h(x)}{p(x)} \mathbf{q}(x)
ight)$$
 where $h \in G_{b,m}$

is called a **polynomial lattice point set** $\mathcal{P}(\mathbf{q}, p)$.

Definition (Niederreiter 1992)

For $s, m \in \mathbb{N}$, choose $p \in \mathbb{Z}_b[x]$ with deg(p) = m, and $\mathbf{q} \in \mathbb{Z}_b[x]^s$. The point set consisting of the b^m points

$$\mathbf{x}_h =
u_m \left(rac{h(x)}{p(x)} \mathbf{q}(x)
ight) \; \; ext{where} \; h \in G_{b,m}$$

is called a **polynomial lattice point set** $\mathcal{P}(\mathbf{q}, p)$.

Dual polynomial lattice

$$\mathcal{D} = \{\mathbf{h} \in G_{b,m}^s : \mathbf{q} \cdot \mathbf{h} \equiv 0 \pmod{p}\}$$

Definition (Niederreiter 1992)

For $s, m \in \mathbb{N}$, choose $p \in \mathbb{Z}_b[x]$ with deg(p) = m, and $\mathbf{q} \in \mathbb{Z}_b[x]^s$. The point set consisting of the b^m points

$$\mathbf{x}_h =
u_m \left(rac{h(x)}{p(x)} \mathbf{q}(x)
ight)$$
 where $h \in G_{b,m}$

is called a **polynomial lattice point set** $\mathcal{P}(\mathbf{q}, \mathbf{p})$.

Dual polynomial lattice

$$\mathcal{D} = \{\mathbf{h} \in G_{b,m}^s : \mathbf{q} \cdot \mathbf{h} \equiv 0 \pmod{p}\}$$

 $\mathcal{P}(\mathbf{q}, p)$ are the polynomial versions of good lattice point sets.

Theorem (Niederreiter 1992)

 $\mathcal{P}(\mathbf{q}, p)$ is a digital (t, m, s)-net over \mathbb{Z}_b with generating matrices C_1, \ldots, C_s , where

$$C_{i} = \begin{pmatrix} u_{1}^{(i)} & u_{2}^{(i)} & \dots & u_{m}^{(i)} \\ u_{2}^{(i)} & u_{3}^{(i)} & \dots & u_{m+1}^{(i)} \\ \vdots & \vdots & & \vdots \\ u_{m}^{(i)} & u_{m+1}^{(i)} & \dots & u_{2m-1}^{(i)} \end{pmatrix} \text{ for } \frac{q_{i}(x)}{p(x)} = \sum_{\ell=w_{i}}^{\infty} \frac{u_{\ell}^{(i)}}{x^{\ell}}$$

and

$$t = m - s + 1 - \min_{\mathbf{h} \in \mathcal{D} \setminus \{\mathbf{0}\}} \sum_{i=1}^{s} \deg(h_i).$$

(Polynomial) lattice point sets: an example



left: N = 987, $\mathbf{g} = (1, 610)$ right: $p(x) = x^{10} + x^8 + x^4 + x^2 + 1$, $\mathbf{q} = (1, x^9 + x^5 + x)$ in $\mathbb{Z}_2[x]$

Three methods for estimating the star discrepancy of $\mathcal{P}(\mathbf{q}, p)$:

Three methods for estimating the star discrepancy of $\mathcal{P}(\mathbf{q}, p)$: Discrepancy estimate based on

• the quality parameter *t*;

Three methods for estimating the star discrepancy of $\mathcal{P}(\mathbf{q}, p)$: Discrepancy estimate based on

- the quality parameter *t*;
- a Erdős-Turan-Koksma type inequality for Walsh functions (Niederreiter 1986, Hellekalek 1994);

Three methods for estimating the star discrepancy of $\mathcal{P}(\mathbf{q}, p)$: Discrepancy estimate based on

- the quality parameter *t*;
- a Erdős-Turan-Koksma type inequality for Walsh functions (Niederreiter 1986, Hellekalek 1994);
- the digital construction.

Theorem (Larcher, Lauss, Niederreiter, Schmid 1996)

Let $m \in \mathbb{N}$ large enough and let $p \in \mathbb{Z}_b[x]$ be irreducible with $\deg(p) = m$. Then there exists $\mathbf{q} \in G_{b,m}^s$ such that

$$t \leq 1 + \log_b \frac{m^{s-1}}{(s-1)!}$$

Theorem (Larcher, Lauss, Niederreiter, Schmid 1996)

Let $m \in \mathbb{N}$ large enough and let $p \in \mathbb{Z}_b[x]$ be irreducible with $\deg(p) = m$. Then there exists $\mathbf{q} \in G_{b,m}^s$ such that

$$t \leq 1 + \log_b rac{m^{s-1}}{(s-1)!}$$

Theorem (Niederreiter 1987)

If \mathcal{P} is a (t, m, s)-net in base b, then

$$D^*_{b^m}(\mathcal{P})\ll_{s,b} b^t rac{m^{s-1}}{b^m}.$$

Hence

$$D^*_{b^m}(\mathcal{P}(\mathbf{q},p)) \ll_{s,b} rac{m^{2s-2}}{b^m} \quad \left(=rac{(\log N)^{2s-2}}{N}
ight).$$

Hence

$$D^*_{b^m}(\mathcal{P}(\mathbf{q},p)) \ll_{s,b} rac{m^{2s-2}}{b^m} \quad \left(=rac{(\log N)^{2s-2}}{N}
ight).$$

For dimension s = b = 2 and for any $m \in \mathbb{N}$ let

$$g_m(x) = \sum_{j=0}^{\lfloor \log_2 m
floor + 1} x^{m - \lfloor m/2^j
floor} \in \mathbb{Z}_2[x] \text{ and } \mathbf{g}_m = (1, g_m).$$

Hence

$$D^*_{b^m}(\mathcal{P}(\mathbf{q}, p)) \ll_{s,b} rac{m^{2s-2}}{b^m} \quad \left(=rac{(\log N)^{2s-2}}{N}
ight).$$

For dimension s = b = 2 and for any $m \in \mathbb{N}$ let

$$g_m(x) = \sum_{j=0}^{\lfloor \log_2 m
floor + 1} x^{m - \lfloor m/2^j
floor} \in \mathbb{Z}_2[x] \text{ and } \mathbf{g}_m = (1, g_m)$$

Theorem (Niederreiter 1987, 1992; Larcher, P. 2002) For any $m \in \mathbb{N}$, $\mathcal{P}(\mathbf{g}_m, x^m)$ is a digital (0, m, 2)-net over \mathbb{Z}_2 and hence

$$D^*_{2^m}(\mathcal{P}(\mathbf{g}_m, x^m)) \leq \left(rac{m}{3} + rac{9}{19}
ight) rac{1}{2^m} \quad \left(\ll rac{\log N}{N}
ight).$$

Theorem (Niederreiter 1992; Dick, Leobacher, P. 2005; Dick, Kritzer, Leobacher, P. 2007)

$$D^*_{b^m}(\mathcal{P}(\mathbf{q},p)) \leq rac{s}{b^m} + R_b(\mathbf{q},p),$$

where

$$R_b(\mathbf{q}, p) = \sum_{\mathbf{h} \in \mathcal{D} \setminus \{\mathbf{0}\}} \prod_{i=1}^s r_b(h_i),$$

where for $h \in G_{b,m}$

$$r_b(h) := \begin{cases} 1 & \text{if } h = 0, \\ \frac{1}{b^{r+1}\sin(\pi\kappa_r/b)} & \text{if } h = \kappa_0 + \kappa_1 x + \dots + \kappa_r x^r, \ \kappa_r \neq 0. \end{cases}$$

Theorem (Niederreiter 1992; Dick, Leobacher, P. 2005; Dick, Kritzer, Leobacher, P. 2007)

For (irreducible) $p \in \mathbb{Z}_b[x]$ with $\deg(p) = m$ there exists a vector $\mathbf{q} \in G_{b,m}^s$ with

$$\mathsf{R}_b(\mathbf{q}, \mathbf{\textit{p}}) \leq rac{1}{b^m-1} \left(1+mrac{b^2-1}{3b}
ight)^s$$

and hence

$$D^*_{b^m}(\mathcal{P}(\mathbf{q},p)) \ll_{s,b} rac{m^s}{b^m} \quad \left(=rac{(\log N)^s}{N}
ight).$$

Such a q can be constructed with a component-by-component algorithm.

Theorem (Niederreiter 1992; Dick, Leobacher, P. 2005; Dick, Kritzer, Leobacher, P. 2007)

For (irreducible) $p \in \mathbb{Z}_b[x]$ with $\deg(p) = m$ there exists a vector $\mathbf{q} \in G_{b,m}^s$ with

$$\mathsf{R}_b(\mathbf{q}, p) \leq rac{1}{b^m-1} \left(1+mrac{b^2-1}{3b}
ight)^s$$

and hence

$$D_{b^m}^*(\mathcal{P}(\mathbf{q},p)) \ll_{s,b} \frac{m^s}{b^m} \quad \left(=\frac{(\log N)^s}{N}\right).$$

Such a **q** can be constructed with a component-by-component algorithm.

The fast cbc-approach requires only $O(smb^m)$ operations (Nuyens and Cools 2006).

Theorem (Kritzer, P. 2010) For any $p \in \mathbb{Z}_b[x]$ with deg(p) = m and any $\mathbf{q} \in (G_{b,m} \setminus \{0\})^s$ we have $R_b(\mathbf{q}, p) \gg_{s,b} b^{\deg(\delta_s)} \frac{(m - \deg(\delta_s))^s}{b^m}$, where $\delta_s := \gcd(q_1, \dots, q_s, p)$.

Theorem (Kritzer, P. 2010)

For any $p \in \mathbb{Z}_b[x]$ with deg(p) = m and any $\mathbf{q} \in (G_{b,m} \setminus \{0\})^s$ we have

$$R_b(\mathbf{q},p) \gg_{s,b} b^{\deg(\delta_s)} rac{(m-\deg(\delta_s))^s}{b^m},$$

where $\delta_s := \gcd(q_1, \ldots, q_s, p)$.

Hence

$$R_b(\mathbf{q},p) \asymp_{s,b} rac{m^s}{b^m} \quad \left(=rac{(\log N)^s}{N}
ight).$$

Theorem (Larcher 1993; Kritzer, P. 2011) For any $p \in \mathbb{Z}_{b}[x]$ with the property • $p(x) = x^m$; or • gcd(p, x) = 1 and deg(p) = mthere exists a generating vector $\mathbf{q} \in G_{b,m}^{s}$ such that $D_{b^m}^*(\mathcal{P}(\mathbf{q},p)) \ll_{s,b} \frac{m^{s-1}\log m}{b^m} \quad \left(=\frac{(\log N)^{s-1}\log\log N}{N}\right).$

Sketch of Proof (rather technical): Let C_1, \ldots, C_s be the generating matrices of $\mathcal{P}(\mathbf{q}, p)$.

Sketch of Proof (rather technical): Let C_1, \ldots, C_s be the generating matrices of $\mathcal{P}(\mathbf{q}, p)$.

Show that



where h(w + 1) depends on $\mathbf{p} \in \mathbb{N}^w$ and on C_{w+1} .

Sketch of Proof (rather technical): Let C_1, \ldots, C_s be the generating matrices of $\mathcal{P}(\mathbf{q}, p)$.

Show that



where h(w + 1) depends on $\mathbf{p} \in \mathbb{N}^w$ and on C_{w+1} .

• Define a set H of q such that h(w + 1) is "large" for all w.

Sketch of Proof (rather technical): Let C_1, \ldots, C_s be the generating matrices of $\mathcal{P}(\mathbf{q}, p)$.

Show that



where h(w + 1) depends on $\mathbf{p} \in \mathbb{N}^w$ and on C_{w+1} .

- Define a set H of q such that h(w + 1) is "large" for all w.
- Show that *H* contains enough polynomials; $|H| \ge b^{s(m-1)}/2$.

Sketch of Proof (rather technical): Let C_1, \ldots, C_s be the generating matrices of $\mathcal{P}(\mathbf{q}, p)$.

Show that



where h(w + 1) depends on $\mathbf{p} \in \mathbb{N}^w$ and on C_{w+1} .

- Define a set H of q such that h(w+1) is "large" for all w.
- Show that H contains enough polynomials; $|H| \ge b^{s(m-1)}/2$.
- Average the discrepancy bound over all $\mathbf{q} \in \mathbf{H}$.

Summary of the three methods:

Method 1: based on t yields optimal discrepancy bound and a construction for s = 2, but not for s > 2;

Summary of the three methods:

- Method 1: based on t yields optimal discrepancy bound and a construction for s = 2, but not for s > 2;
- Method 2: based on R_b yields a good discrepancy bound for any $s \ge 2$ together with a reasonable fast construction;

Summary of the three methods:

- Method 1: based on t yields optimal discrepancy bound and a construction for s = 2, but not for s > 2;
- Method 2: based on R_b yields a good discrepancy bound for any $s \ge 2$ together with a reasonable fast construction;
- Method 3: based on C_1, \ldots, C_s yields the currently best discrepancy bounds for $s \ge 3$, but no construction.

Open question

Open question

For $s \geq 3$, do there exist $\mathcal{P}(\mathbf{q}, p)$ such that

$$D_{b^m}^*(\mathcal{P}(\mathbf{q},p)) \ll_{s,b} rac{m^{s-1}}{b^m} \quad \left(=rac{(\log N)^{s-1}}{N}
ight)?$$

Open question

Open question

For $s \geq 3$, do there exist $\mathcal{P}(\mathbf{q}, p)$ such that

$$D^*_{b^m}(\mathcal{P}(\mathbf{q},p)) \ll_{s,b} rac{m^{s-1}}{b^m} \quad \left(=rac{(\log N)^{s-1}}{N}
ight)$$

Computer experiments (s = 3): $\mathbf{g}_m = (1, g_m)$ can be extended to $\mathbf{g}'_m = (1, g_m, f_m)$ such that $\mathcal{P}(\mathbf{g}'_m, x^m)$ is a digital (2, m, 3)-net over \mathbb{Z}_2 . This would mean that

$$D_{2^m}^*(\mathcal{P}(\mathbf{g}_m', x^m)) \leq \frac{m^2 - 2m + 9}{2^m} \quad \left(\ll \frac{(\log N)^2}{N} \right)$$

The weighted star discrepancy

Let $\gamma = (\gamma_1, \gamma_2, \ldots) \in \mathbb{R}^{\infty}_+$ (weights). For $\mathfrak{u} \subseteq \{1, \ldots, s\}$ let $\gamma_{\mathfrak{u}} = \prod_{i \in \mathfrak{u}} \gamma_i$.
The weighted star discrepancy

Let $\gamma = (\gamma_1, \gamma_2, \ldots) \in \mathbb{R}^{\infty}_+$ (weights). For $\mathfrak{u} \subseteq \{1, \ldots, s\}$ let $\gamma_{\mathfrak{u}} = \prod_{i \in \mathfrak{u}} \gamma_i$.

Weighted star discrepancy (Sloan and Woźniakowski 1998) The weighted star discrepancy is given by

$$D^*_{N,\gamma}(\mathcal{P}) = \sup_{\mathbf{z} \in [0,1]^s} \max_{\emptyset \neq \mathfrak{u} \subseteq \{1,...,s\}} \gamma_{\mathfrak{u}} |\Delta_{\mathcal{P}_{\mathfrak{u}}}(\mathbf{z})|.$$

The weighted star discrepancy

Let $\gamma = (\gamma_1, \gamma_2, \ldots) \in \mathbb{R}^{\infty}_+$ (weights). For $\mathfrak{u} \subseteq \{1, \ldots, s\}$ let $\gamma_{\mathfrak{u}} = \prod_{i \in \mathfrak{u}} \gamma_i$.

Weighted star discrepancy (Sloan and Woźniakowski 1998)

The weighted star discrepancy is given by

$$D^*_{N,\gamma}(\mathcal{P}) = \sup_{\mathsf{z} \in [0,1]^s} \max_{\emptyset \neq \mathfrak{u} \subseteq \{1,...,s\}} \gamma_{\mathfrak{u}} |\Delta_{\mathcal{P}_{\mathfrak{u}}}(\mathsf{z})|.$$

Weighted Koksma-Hlawka inequality

 $|I_s(f) - Q_{N,s}(f)| \leq D^*_{N,\gamma}(\mathcal{P}) ||f||_{s,\gamma}.$

Tractability

Discrepancy bounds of the form



Figure: The function $N \mapsto (\log N)^s / N$ is increasing for $N \leq e^s$ (here s = 10).

Tractability

For $s \in \mathbb{N}$ and $\varepsilon > 0$ define

 $N_{\gamma}(s,\varepsilon) = \min\{N \in \mathbb{N} \, : \, \exists \mathcal{P} \subseteq [0,1)^s, |\mathcal{P}| = N \text{ and } D^*_{N,\gamma}(\mathcal{P}) \leq \varepsilon\}.$

Tractability

For $s \in \mathbb{N}$ and $\varepsilon > 0$ define

 $N_{\gamma}(s,\varepsilon) = \min\{N \in \mathbb{N} \, : \, \exists \mathcal{P} \subseteq [0,1)^s, |\mathcal{P}| = N \text{ and } D^*_{N,\gamma}(\mathcal{P}) \leq \varepsilon\}.$

Tractability

The weighted star discrepancy is called **polynomially tractable**, if $\exists C, \alpha, \beta > 0$ such that

$$N_{\gamma}(s,\varepsilon) \leq Cs^{lpha}\varepsilon^{-eta} \ \ \forall s \in \mathbb{N}, \ \ \forall \varepsilon \in (0,1).$$

If $\alpha = 0$, then $D^*_{N,\gamma}$ is said to be **strongly tractable**. The infimum of β for which $\exists C > 0$ such that $N_{\gamma}(s, \varepsilon) \leq C \varepsilon^{-\beta}$ is called the ε -exponent of strong tractability.

The weighted star discrepancy

Theorem (Dick, Leobacher, P. 2005 and Dick, Leobacher, Kritzer, P. 2007)

$$D^*_{b^m, oldsymbol{\gamma}}(\mathcal{P}(\mathbf{q}, oldsymbol{p})) \leq \sum_{\emptyset
eq \mathfrak{u} \subseteq \{1, ..., s\}} \gamma_\mathfrak{u} \left(1 - \left(1 - rac{1}{b^m}
ight)^{|\mathfrak{u}|}
ight) + R_{b, oldsymbol{\gamma}}(\mathbf{q}, oldsymbol{p}),$$

where

$$R_{b,\gamma}(\mathbf{q},p) = \sum_{\mathbf{h}\in\mathcal{D}\setminus\{\mathbf{0}\}}\prod_{i=1}^{s}r_{b}(h_{i},\gamma_{i}).$$

Here for $h \in G_{b,m}$ we put

$$r_b(h,\gamma) = \begin{cases} 1+\gamma & \text{if } h=0, \\ \gamma r_b(h) & \text{if } h \neq 0. \end{cases}$$

 $R_{b,\gamma}(\mathbf{q},p)$ can be computed in $O(b^m s)$ operations.

CBC-algorithm

Given a prime $b, s, m \in \mathbb{N}$, $p \in \mathbb{Z}_b[x]$, with deg(p) = m, and weights $\gamma = (\gamma_i)_{i \ge 1}$.

CBC-algorithm

Given a prime $b, s, m \in \mathbb{N}$, $p \in \mathbb{Z}_b[x]$, with deg(p) = m, and weights $\gamma = (\gamma_i)_{i \ge 1}$.

• Choose $q_1 = 1$.

CBC-algorithm

Given a prime $b, s, m \in \mathbb{N}$, $p \in \mathbb{Z}_b[x]$, with deg(p) = m, and weights $\gamma = (\gamma_i)_{i \ge 1}$.

• Choose $q_1 = 1$.

 For d > 1, assume we have already constructed q₁,..., q_{d-1} ∈ G^{*}_{b,m}. Then find q_d ∈ G^{*}_{b,m} which minimises the quantity

 $R_{b,\gamma}((q_1,\ldots,q_{d-1},q_d),p)$

as a function of q_d .

CBC-algorithm

Given a prime $b, s, m \in \mathbb{N}$, $p \in \mathbb{Z}_b[x]$, with deg(p) = m, and weights $\gamma = (\gamma_i)_{i \ge 1}$.

• Choose $q_1 = 1$.

 For d > 1, assume we have already constructed q₁,..., q_{d-1} ∈ G^{*}_{b,m}. Then find q_d ∈ G^{*}_{b,m} which minimises the quantity

$$R_{b,\gamma}((q_1,\ldots,q_{d-1},q_d),p)$$

as a function of q_d .

• The cost for the CBC-algorithm is of $O(b^{2m}s^2)$ operations.

CBC-algorithm

Given a prime $b, s, m \in \mathbb{N}$, $p \in \mathbb{Z}_b[x]$, with deg(p) = m, and weights $\gamma = (\gamma_i)_{i \ge 1}$.

• Choose $q_1 = 1$.

 For d > 1, assume we have already constructed q₁,..., q_{d-1} ∈ G^{*}_{b,m}. Then find q_d ∈ G^{*}_{b,m} which minimises the quantity

$$R_{b,\gamma}((q_1,\ldots,q_{d-1},q_d),p)$$

as a function of q_d .

- The cost for the CBC-algorithm is of $O(b^{2m}s^2)$ operations.
- Nuyens and Cools (2006) introduced the Fast CBC-construction with a significant reduction of cost to O(smb^m) operations with O(b^m) memory space.

Theorem (Dick, Leobacher, P. 2005; Dick, Kritzer, Leobacher, P. 2007)

If $\mathbf{q} \in (G^*_{b,m})^s$ is constructed with the CBC-algorithm. Then

$$R_{b,\gamma}(\mathbf{q},p) \leq rac{1}{b^m-1}\prod_{i=1}^s \left(1+\gamma_i\left(1+mrac{b^2-1}{3b}
ight)
ight),$$

Theorem (Dick, Leobacher, P. 2005; Dick, Kritzer, Leobacher, P. 2007)

If $\mathbf{q} \in (G^*_{b,m})^s$ is constructed with the CBC-algorithm. Then

$$\mathsf{R}_{b,\gamma}(\mathbf{q}, p) \leq rac{1}{b^m-1} \prod_{i=1}^s \left(1+\gamma_i \left(1+mrac{b^2-1}{3b}
ight)
ight),$$

Corollary

If $\sum_{i=0}^{\infty} \gamma_i < \infty$, then for any $\delta > 0$ there exists $c_{\gamma,\delta} > 0$, such that

$$D^*_{b^m, oldsymbol{\gamma}}(\mathcal{P}(\mathbf{q}, p)) \leq rac{c_{oldsymbol{\gamma}, \delta}}{b^{m(1-\delta)}}.$$

• Let $N = 2^{m_1} + \cdots + 2^{m_k}$, where $0 \le m_1 < m_2 < \ldots < m_k$.

- Let $N = 2^{m_1} + \cdots + 2^{m_k}$, where $0 \le m_1 < m_2 < \ldots < m_k$.
- For $1 \le j \le k$ choose $p^{(j)} \in \mathbb{Z}_2[x]$ with $\deg(p^{(j)}) = m_j$ and construct $\mathbf{q}^{(j)} \in G^s_{2,m_i}$ with the CBC-algorithm.

- Let $N = 2^{m_1} + \cdots + 2^{m_k}$, where $0 \le m_1 < m_2 < \ldots < m_k$.
- For $1 \le j \le k$ choose $p^{(j)} \in \mathbb{Z}_2[x]$ with $\deg(p^{(j)}) = m_j$ and construct $\mathbf{q}^{(j)} \in G^s_{2,m_i}$ with the CBC-algorithm.
- Set $\mathcal{P}_N = \mathcal{P}(\mathbf{q}^{(1)}, p^{(1)}) \cup \ldots \cup \mathcal{P}(\mathbf{q}^{(k)}, p^{(k)}).$

- Let $N = 2^{m_1} + \cdots + 2^{m_k}$, where $0 \le m_1 < m_2 < \ldots < m_k$.
- For $1 \le j \le k$ choose $p^{(j)} \in \mathbb{Z}_2[x]$ with $\deg(p^{(j)}) = m_j$ and construct $\mathbf{q}^{(j)} \in G^s_{2,m_i}$ with the CBC-algorithm.
- Set $\mathcal{P}_N = \mathcal{P}(\mathbf{q}^{(1)}, p^{(1)}) \cup \ldots \cup \mathcal{P}(\mathbf{q}^{(k)}, p^{(k)}).$

Theorem (Hinrichs, P., Schmid 2008)

If $\sum_{i=0}^{\infty} \gamma_i < \infty$, then for any $\delta > 0$ there exists $C_{\gamma,\delta} > 0$, such that

$$D^*_{N,\gamma}(\mathcal{P}_N) \leq rac{C_{\gamma,\delta}}{N^{1-\delta}}.$$

- Let $N = 2^{m_1} + \cdots + 2^{m_k}$, where $0 \le m_1 < m_2 < \ldots < m_k$.
- For $1 \le j \le k$ choose $p^{(j)} \in \mathbb{Z}_2[x]$ with $\deg(p^{(j)}) = m_j$ and construct $\mathbf{q}^{(j)} \in G^s_{2,m_i}$ with the CBC-algorithm.
- Set $\mathcal{P}_N = \mathcal{P}(\mathbf{q}^{(1)}, p^{(1)}) \cup \ldots \cup \mathcal{P}(\mathbf{q}^{(k)}, p^{(k)}).$

Theorem (Hinrichs, P., Schmid 2008)

If $\sum_{i=0}^{\infty} \gamma_i < \infty$, then for any $\delta > 0$ there exists $C_{\gamma,\delta} > 0$, such that

$$D^*_{N,\gamma}(\mathcal{P}_N) \leq rac{C_{\gamma,\delta}}{N^{1-\delta}}.$$

The weighted star discrepancy is **strongly tractable** with ε -exponent equal to one.