Answer to selected exercises

1 Answer to Exercise 8.2

We provide an answer to Exercise 8.2. To better illustrate the connection between Sobol and generalized Niederreiter sequences, we consider a special case first.

1.1 First coordinate of Sobol and Niederreiter sequence

We use the notation from [1, Section 8.1]. Since the constructions of Sobol and Niederreiter sequences are coordinate-wise, it suffices to consider only one coordinate and we can drop the index \( i \) from the notation.

1.1.1 Niederreiter sequence

We consider the special case \( p = 1 + x \). Then \( e = 1 \).

We have

\[
\frac{1}{1 + x} = \frac{1}{x} + \frac{1}{x^2} + \cdots \in \mathbb{Z}_2((x^{-1}))
\]

since in \( \mathbb{Z}_2((x^{-1})) \) we have \( x^{-j} + x^{-j} \equiv 0 \). Further

\[
\frac{1}{(1 + x)^j} = \sum_{r=0}^{\infty} \binom{r + j - 1}{j - 1} \frac{1}{x^{j+r}} = \sum_{r=j-1}^{\infty} \binom{r}{j-1} \frac{1}{x^{r+1}}.
\]

The generating matrix \( C = (c_{j,r})_{j \geq 1, r \geq 0} \) is given by

\[
c_{j,r} = \binom{r}{j-1} \pmod{2},
\]

where \( \binom{r}{j-1} = 0 \) for \( r < j - 1 \).

1.1.2 Sobol sequence

The Sobol sequence is a digital sequence with generating matrix \( C = (c_{j,r})_{j \geq 1, r \geq 0} \). In the following we find the entries \( c_{j,r} \) of the generating matrix.

Choose odd natural numbers \( m_k \) such that \( m_k < 2^k \) for \( 1 \leq k \leq e \). Let the binary representation of \( m_k \) be given as \( m_k = m_{k,0} + m_{k,1}2 + \cdots + m_{k,k-1}2^{k-1} \) with \( m_{k,j} \in \{0, 1\} \) and \( m_{k,0} = 1 \). The construction of \( m_k \) for \( k > e \) implies that we also have \( m_k < 2^k \) and \( m_k \) odd for \( k > e \).

The generating matrix of the Sobol sequence is given by \( C = (\vec{v}_1, \vec{v}_2, \vec{v}_3, \ldots) \in \mathbb{Z}_2^{N \times N} \), where \( \vec{v}_k = (m_{k,k-1}, m_{k,k-2}, \ldots, m_{k,0}, 0, \ldots)^\top \)

\[
v_k = \frac{m_k}{2^k} = m_{k,k-1}2^{-1} + m_{k,k-2}2^{-2} + \cdots + m_{k,0}2^{-k}.
\]
Thus for any $j \geq 1$ and $r \geq 0$ we have

$$c_{j,r} = m_{r+1,r-j+1}.$$  

We consider the special case $p(x) = 1 + x$. Then $e = 1$ and $m_1 = 1$. We have

$$m_{r+1} = 2m_r \oplus m_r$$

$$= m_{r,0} + (m_{r,1} \oplus m_{r,0})2 + \cdots + (m_{r,r-1} \oplus m_{r,r-2})2^{r-1} + m_{r,r-1}2^r,$$

where $m_{r,z} \oplus m_{r,z-1}$ denotes the addition modulo 2. Thus

$$m_{r+1,z} = m_{r,z} + m_{r,z-1} \pmod{2},$$

where we set $m_{r,r} = m_{r,r-1} = 0$.

In order for the generating matrices for the Niederreiter and Sobol sequence to be identical, we need to show that

$$c_{j,r} = m_{r+1,r-j+1} = \binom{r}{j-1} = \binom{r}{r-j+1} \pmod{2},$$

or equivalently, that

$$m_{r+1,z} = \binom{r}{z} \pmod{2}.$$  

This follows by induction on $r$. For $r = 0$ we have $m_{1,0} = 1$ and $m_{r,z} = 0$ otherwise. Assume we have $m_{r,z} = \binom{r-1}{z} \pmod{2}$ for all $z \geq 0$. Then

$$m_{r+1,z} = m_{r,z} + m_{r,z-1} = \binom{r}{z} + \binom{r-1}{z-1} = \binom{r}{z} \pmod{2}.$$  

### 1.2 The general case

We consider now the general case. Let

$$p(x) = x^e + a_1x^{e-1} + a_2x^{e-2} + \cdots + a_{e-1}x + 1.$$  

For $r \geq e$ we have

$$m_{r+1} = 2a_1m_r \oplus \cdots \oplus 2^{e-1}a_{e-1}m_{r+2-e} \oplus 2^em_{r+1-e} \oplus m_{r+1-e},$$

where here $\oplus$ is the bit-by-bit exclusive-or operator (digitwise addition modulo 2). Using $m_k = m_{k,0} + m_{k,1}2 + \cdots + m_{k,k-1}2^{k-1}$ with $m_{k,j} \in \{0, 1\}$ we therefore have

$$m_{r+1,z} = a_1m_{r,z-1} + a_2m_{r-1,z-2} + \cdots + a_{e-1}m_{r+2-e,z-1} + m_{r+1-e,z-1} + m_{r+1-e,z} \pmod{2}. \quad (1)$$

From above we have that the entries of the corresponding generating matrix $C = (c_{j,r})_{j \geq 1, r \geq 0}$ are given by

$$c_{j,r} = m_{r+1,r+1-j}. \quad (2)$$

Thus (1) and (2) imply that

$$c_{j,r} = a_1c_{j,r-1} + a_2c_{j,r-2} + \cdots + a_{e-1}c_{j,r+1-e} + c_{j,r-e} + c_{j-e,r-e} \pmod{2}, \quad (3)$$
where \( c_{j-e,r-e} = 0 \) for \( 1 \leq j \leq e \).

For fixed \( 1 \leq j \leq e \), the sequence \((c_{j,r})_{r \geq 0}\) is a linear recurring sequence (see [2, Chapter 8]) with characteristic polynomial \( p(x) \). Define

\[
G_j(x) = \sum_{r=0}^{\infty} c_{j,r} x^r.
\]

By [2, Theorem 8.40] we have

\[
G_j(x) = \frac{g_j(x)}{p^*(x)},
\]

where \( p^*(x) = x^e p(1/x) \) is the reciprocal characteristic polynomial and where \( g_j(x) \) are polynomials of degree at most \( e - 1 \). A formula for the polynomials \( g_j(x) \) is also given in [2, Theorem 8.40].

Let

\[
y_{1,j}(x) = x^{e-1} g_j(1/x) \quad \text{for} \quad 1 \leq j \leq e.
\]

Note that the \( y_{1,j}(x) \) are polynomials of degree at most \( e - 1 \). Then

\[
\frac{y_{1,j}(x)}{p(x)} = \frac{x^{e-1} g_j(1/x)}{p(x)} = \frac{x^e g_j(1/x)}{x^e p^*(1/x)} = \frac{1}{x} G_j(1/x) = \sum_{r=0}^{\infty} c_{j,r} x^{-r-1}.
\]

This is now just the construction from the generalized Niederreiter sequence.

Let now \( e < j \leq 2e \). For the generalized Niederreiter sequence we have

\[
\frac{1}{x} G_j(1/x) = \sum_{r=0}^{\infty} c_{j,r} x^{-r-1} = \frac{y_{1,j-e}(x)}{p^2(x)}.
\]

On the other hand, we have

\[
\frac{y_{1,j-e}(x)}{p^2(x)} = \frac{1}{p(x)} \frac{y_{1,j-e}(x)}{p(x)} = \frac{1}{xp(x)} G_{j-e}(1/x).
\]

Thus in order that Sobol’s and generalized Niederreiter’s construction are the same, we must have

\[
\frac{1}{x} G_j(1/x) = \frac{1}{xp(x)} G_{j-e}(1/x),
\]

or equivalently

\[
p^*(x)G_j(x) = x^e p(1/x) G_j(x) = x^e G_{j-e}(x).
\]

The last equation can be rewritten as

\[
(1 + a_1 x + a_2 x^2 + \cdots + a_{e-1} x^{e-1} + x^e) \sum_{r=0}^{\infty} c_{j,r} x^r = \sum_{r=0}^{\infty} c_{j-e,r} x^{r+e}.
\]

By comparing coefficients the last equation is equivalent to

\[
c_{j,r} + a_1 c_{j,r-1} + a_2 c_{j,r-2} + \cdots + a_{e-1} c_{j,r-e+1} + c_{j,r-e} = c_{j-e,r-e} \pmod{2}.
\]

This holds since this expression is the same as (3).

The case where \( j > 2e \) can be shown in a similar fashion.
References
