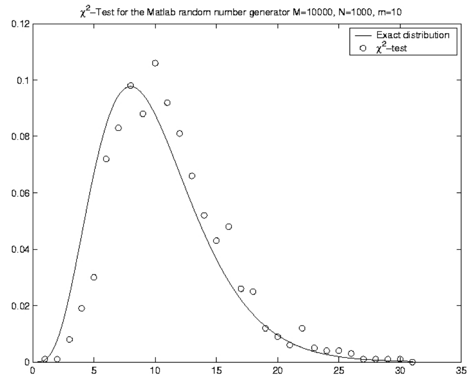

Figure 2.2: A χ^2-test for the random number generator of MATLAB. Obviously, the test was succesful.

Example 2.2.1 *Figure 2.2 shows the result of a χ^2-test for the random number generator of* MATLAB*. The code for the χ^2-test is also written in* MATLAB*.*

2.2.2 Gaps

Definition 2.2.2 *For a given interval $J \subset [0,1]$ a sequence $(t_n)_{n\in\mathbb{N}_0}$ is said to have a* gap of length k*, if there exists some $n \in \mathbb{N}_0$ such that $t_n, \ldots, t_{n+k-1} \notin J$, but $t_{n+k} \in J$.* $\square$

For a corresponding test, choose $h \in \mathbb{N}$, and count the number of gaps of length $0, 1, \ldots, h-1, h$. On this sequence of pseudo random numbers, the above χ^2-test is applied.

For further information on random number generation and corresponding tests, we refer to [10].

2.3 Discrepancy

We have seen statistical tests to check the distribution of pseudo random numbers. We have concentrated on the uniform distribution. So far, we do not have a *measure* how good a uniform distribution is matched. We will now introduce such a measure.

Definition 2.3.1 *Let $X := \{x_1, \ldots, x_N\} \subset [0,1]^m$ be a sequence of normalized pseudo random vectors.*

(a) Let $\mathcal{Q}$ be the set of all quads in $[0,1]^m$. Then, we call

$$D(X) := \sup_{Q \in \mathcal{Q}} \left| \frac{\#\{x_i \in X : x_i \in Q\}}{\#X} - \text{vol } (Q) \right|$$

the extreme discrepancy *of X.*

(b) For $X = \{x_1, x_2, \ldots\}$, we also use the abbreviation

$$D_N := D(\{x_1, \ldots, x_N\}).$$

If $\lim_{N\to\infty} D_N = 0$, then we say that X consists of uniformly distributed *points.* □

The idea behind the latter definition is that for a set of uniformly distributed points the portion of those points lying in a quad Q should at least almost correspond to the volume of Q. Of course the quantity $D(X)$ is not so easy to compute since the determination of the supremum over all quads might be a delicate and in particular expensive task. Thus, one also considers the following measure.

Definition 2.3.2 *Let $Q^* = \prod_{i=1}^{m} [0, y_i)$, $0 < y_i \leq 1$, be a quad with one corner in 0 and denote by $\mathcal{Q}^*$ the set of all these quads. Then, the quantity*

$$D^*(X) := \sup_{Q^* \in \mathcal{Q}^*} \left| \frac{\#\{x_i \in X : x_i \in Q^*\}}{\#X} - \ vol\ (Q^*) \right|$$

is called star discrepancy *of X.* □

Obviously, the star discrepancy is easier to access. The next result shows that it is in fact an approximation of the discrepancy.

Proposition 2.3.3 *The following estimates hold*

(a) $0 \leq D_N \leq 1$,

(b) $D_N^* \leq D_N \leq 2^m D_N^*$,

(c) $D_N^* \geq \frac{1}{2N}$ *for* $m = 1$.

Proof: We leave the proof as an easy exercise. $\square$

In Definition 2.3.1 (b) we just require that D_N tends to zero for $N \to \infty$. This is a statement of pure asymptotic character. In practice one is of course also interested that already a moderate number of pseudo random numbers is almost uniformly distributed. Hence, one is interested how fast D_N tends to zero, i.e., what is the rate of decay. This is reflected by the following definition.

Definition 2.3.4 *A sequence* $(x_k)_{k\in\mathbb{N}} \subset [0,1]^m$ *is called of* low discrepancy *if*

$$D_N \leq C_m \frac{(\log N)^m}{N} \tag{2.3.1}$$

with a constant $0 \leq C_m < \infty$ *independent of* N. *A deterministic sequence of numbers is called a set of* quasi random numbers *if (2.3.1) holds.* $\square$

Remark: In moderate dimensions m, the above estimate basically means

$$D_N \approx \mathcal{O}(N^{-1}).$$

However, the curse of dimensionality shows up due to the term $(\log N)^m$. It is widely believed (see [10], p. 32) that

$$D_N^* \geq B_m \frac{(\log N)^m}{N}$$

with a constant B_m depending only on m. This means that

$$\mathcal{O}(N^{-1}(\log N)^m)$$

would be the optimal rate.

Some examples

Example 2.3.5 *For* $m = 1$ *and* $x_i := \frac{2i-1}{2N}, i = 1, \ldots N$, *we obtain* $D_N^* = \frac{1}{2N}$. *In fact, let* $Q^* = [0, y)$, $0 < y \leq 1$ *so that vol* $(Q^*) = y$ *and*

$$\begin{aligned} x_i \in Q^* \iff \tfrac{2i-1}{2N} < y &\iff 2i - 1 \leq 2Ny \\ &\iff i \leq \tfrac{2Ny+1}{2}. \end{aligned}$$

Hence, we have

$$D^*(X) = \sup_{0<y\le 1} \Big\{ \underbrace{\frac{2Ny+1}{2N} - y}_{=\frac{2Ny+1}{2N} - \frac{2Ny}{2N} = \frac{1}{2N}} \Big\} = \frac{1}{2N}.$$

By Proposition 2.3.3 (c) this is optimal. On the other hand, the sequence (x_i), $i \in \mathbb{N}$ has to be computed for every N from scratch which of course is highly inefficient if N grows. Hence, it would be better if the numbers could be set in a dynamical way that allows for updating. The next example shows one way to achieve this.

Definition 2.3.6 *Let $b \ge 2$ be an integer and for $i \in \mathbb{N}$ consider the b-adic representation of i to the base b, namely*

$$i = \sum_{k=0}^{j} d_k\ b^k\ ,\ d_k \in \{0, 1, \dots, b-1\},$$

where the upper index j of course depends on i (or, on a computer, on the finite arithmetic). Then, the mapping ϕ_b defined by

$$\phi_b(i) := \sum_{k=0}^{j} d_k\ b^{-k-1}$$

is called radical-inverse function. $\square$

The radical-inverse function can be interpreted as a 'reflection at the radix point', i.e., $i \mapsto x \in \mathbb{Q}$, $0 < x < 1$. If the number of digits j in i is increased, the highest power of b is increased which in turns increases the fineness of the rational numbers i, i.e., new numbers are dynamically inserted. Combining different radical-inverse functions yields the following sequence.

The sequence

$$\frac{1}{2}, \frac{1}{4}, \frac{3}{4}, \frac{1}{8}, \frac{5}{8}, \frac{3}{8}, \frac{7}{8}, \frac{1}{16}, \dots$$

known as *van der Corput* sequence can be generated by $x_n := \phi_2(n)$. In general, a sequence defined by

$$x_n := \phi_b(n)$$

is called *van der Corput* sequence. It can be shown that all these sequences are low discrepancy sequences.

An extension to several space dimensions is given by the following definition.

Definition 2.3.7 *Assume that $p_1, \dots, p_m$ are coprime integers. Then, the vectors*

$$x_i := (\phi_{p_1}(i), \dots, \phi_{p_m}(i)) \in \mathbb{R}^m \ , \ i = 1, 2, \dots$$

are called Halton sequence*.*

2.4 Transformed Random Variables

So far we have considered 'only' uniformly distributed quasi random numbers. A (very) simple method to construct an approximately normally distributed sequence of random numbers from a uniformly distributed sequence $U_i \sim \mathcal{U}[0,1]$ is the following

$$X := \sum_{i=1}^{12} U_i - 6.$$

One easily obtains by the central limit theorem that approximately $X \sim \mathcal{N}(0,1)$. Obviously, this is not a very sophisticated method and, as we shall see next, transformation methods are in fact much better.

2.4.1 Inversion

The quite simple idea of this approach is to invert the particular distribution function.

Theorem 2.4.1 *Let $U \sim \mathcal{U}[0,1]$ and F be a uniformly continuous, strictly monotone distribution function. Then there exists the inverse $F^{-1} : [0,1] \to \mathbb{R}$ and $F^{-1}(U)$ is distributed according to F.*

Proof: It is easily seen that for $F^{-1}(z) = x$

$$\begin{aligned} U \sim \mathcal{U}[0,1] \quad &\iff \quad P(U \leq \xi) = \xi \text{ for } 0 \leq \xi \leq 1 \\ &\iff \quad P(F^{-1}(U) \leq x) = P(U \leq F(x)) = F(x). \quad \square \end{aligned}$$

Remark 2.4.2 *The statement of Theorem 2.4.1 also applies for more general distribution functions.*

Even though this straightforward apporach seems to yield the desired result, there is a serious drawback. E.g. for the normal distribution there is no Gaussian error-integral, in particular neither for $F(x)$ nor for $f = F^{-1}(x)$ a closed formula exists. Thus one has to solve the non-linear problem $f(x) = u$