Sobol' Sequences with Guaranteed-Quality 2D Projections

NICOLAS BONNEEL, CNRS, Université Claude Bernard Lyon 1, INSA Lyon, France
DAVID COEURJOLLY, CNRS, Université Claude Bernard Lyon 1, INSA Lyon, France
JEAN-CLAUDE IEHL, Université Claude Bernard Lyon 1, CNRS, INSA Lyon, France
VICTOR OSTROMOUKHOV, Université Claude Bernard Lyon 1, CNRS, INSA Lyon, France

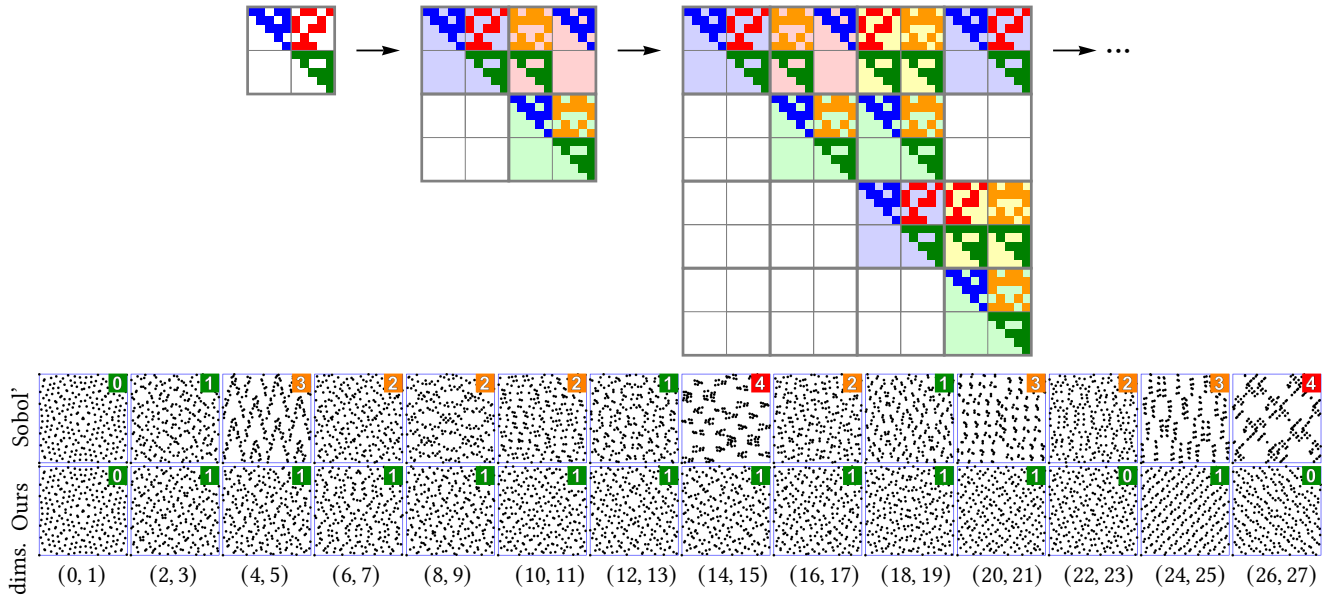


Fig. 1. We demonstrate that 2D Sobol' sequences constructed with polynomials p and p^2+p+1 have a characteristic matrix $K = M_{p^2+p+1}M_p^{-1}$ that can be obtained with a simple recursive algorithm. This is illustrated using polynomials of degrees $e = 5$ and $2e = 10$, where each colored block has dimensions $e \times e$. They produce high-quality $(1, 2)$-sequences (with quality factor $t = 1$) under mild conditions on K's blocks and p (bottom). The quality factor t of each point set is indicated in the upper-right corner of each patch (only 256 points are shown). We use these $(1, 2)$-sequences to construct higher-dimensional low-discrepancy sequences with high-quality 2D and 4D projections.

Low-discrepancy sequences, and more particularly Sobol' sequences are gold standard for drawing highly uniform samples for quasi-Monte Carlo applications. They produce so-called (t, s)-sequences, that is, sequences of s-dimensional samples whose uniformity is controlled by a non-negative integer quality factor t. The Monte Carlo integral estimator has a convergence rate that improves as t decreases. Sobol' construction in base 2 also provides extremely fast sampling point generation using efficient xor-based arithmetic. Computer graphics applications, such as rendering, often require high uniformity in consecutive 2D projections and in higher-dimensional projections at the same time. However, it can be shown that, in the classical Sobol' construction, only a single 2D sequence of points (up to scrambling), constructed using irreducible polynomials x and $x+1$, achieves the ideal $t = 0$ property. Reusing this sequence in projections necessarily loses high dimensional uniformity. We prove the existence and construct many 2D Sobol' sequences having $t = 1$ using irreducible polynomials p and p^2+p+1. They can be readily combined to produce higher-dimensional low discrepancy sequences with a high-quality $t = 1$, guaranteed in consecutive pairs of dimensions. We provide the initialization table that can be directly used with any existing Sobol' implementation, along with the corresponding generator matrices, for an optimized 692-dimensional Sobol' construction. In addition to guaranteeing the $(1, 2)$-sequence property for all consecutive pairs, we ensure that $t \leq 4$ for consecutive 4D projections up to 2^{15} points.

CCS Concepts: • **Mathematics of computing** → **Random number generation**; Computations in finite fields; *Quadrature*; • **Computing methodologies** → *Rendering*.

Additional Key Words and Phrases: Quasi-Monte Carlo, Sobol', low discrepancy sequences, irreducible polynomials

ACM Reference Format:
Nicolas Bonneel, David Coeurjolly, Jean-Claude Iehl, and Victor Ostromoukhov. 2025. Sobol' Sequences with Guaranteed-Quality 2D Projections. *ACM Trans. Graph.* 44, 4 (August 2025), 16 pages. https://doi.org/10.1145/3730821

Authors' Contact Information: Nicolas Bonneel, CNRS, Université Claude Bernard Lyon 1, INSA Lyon, France, nicolas.bonneel@liris.cnrs.fr; David Coeurjolly, CNRS, Université Claude Bernard Lyon 1, INSA Lyon, France, david.coeurjolly@cnrs.fr; Jean-Claude Iehl, Université Claude Bernard Lyon 1, CNRS, INSA Lyon, France, jean-claude.iehl@liris.cnrs.fr; Victor Ostromoukhov, Université Claude Bernard Lyon 1, CNRS, INSA Lyon, France, victor.ostromoukhov@liris.cnrs.fr.

ACM 1557-7368/2025/8-ART
https://doi.org/10.1145/3730821

1 Introduction

Integrating a function using quasi-Monte Carlo consists in evaluating it at well-chosen uniformly distributed sample points, and averaging these values. Sobol' sequences arise as the cornerstone of quasi-Monte Carlo, by producing extremely well-distributed sampling points whose uniformity drastically improves the convergence rate, compared to classical Monte Carlo methods. These points are constructed using a fast and compact recursive algorithm involving polynomials and matrices. Sobol' sequences have thus been widely adopted in computer graphics, notably for rendering where efficiency is paramount. Their mathematical beauty, their connections to Pascal matrices (or Sierpinsky triangle) and Galois theory also make them appealing to the mathematician, but their difficulty comprehending may discourage others. This paper gives new fundamental mathematical insights on Sobol' sequences, exploring particular pairs of polynomials and new Sobol' matrix constructions, with practical and provable benefits in terms of quasi-Monte Carlo integration error.

Sobol' sequences produce a sequence of samples in arbitrary dimension by multiplying Sobol' matrices with a base-b representation of the sample index, where one Sobol' matrix is used per dimension. To compute a Sobol' matrix, a polynomial p of degree e and an initialization matrix of size $e \times e$ (often called *direction vectors* in prior work) are required. The (triangular) Sobol' matrix is recursively constructed column by column, where the next column is computed as a linear combination of the previous e columns weighted by the polynomial coefficients (plus a shifted column), with all operations performed modulo b (or over Galois Field $GF(b)$). The uniformity of the produced sample points is determined by a non-negative integer parameter t, where $t = 0$ corresponds to the best achievable quality, and the quasi-Monte Carlo integral estimator converges with a rate roughly proportional to b^t (see [Lemieux 2009] page 157, and [Niederreiter 1988]).

An s-dimensional set with b^m samples with quality t is called a (t, m, s)-net (see Fig. 2). If such a point set is a (t, m, s)-net for all m, then it is a (t, s)-sequence. We are particularly interested in the case $s = 2$, not only for producing 2D points for 2-dimensional problems, but most importantly to control 2-dimensional projections of higher-dimensional problems [Joe and Kuo 2008] arising for example in computer graphics such as rendering.

It has been demonstrated that, in base $b = 2$, and when considering 2D points, matrices that generate $(0, 2)$-sequences are inherently related by a Pascal matrix [Ahmed et al. 2023; Hofer and Suzuki 2019]. Consequently, the only pair of polynomials that produce $t = 0$ using Sobol' construction are x and $x + 1$. The space of $t = 0$ sequences is thus extremely limited, when $b = 2$. One possible solution is to increase b, as suggested in [Ostromoukhov et al. 2024], which allows for additional polynomials that generate $t = 0$ sequences. However, the effect on the integration error for $t \neq 0$ becomes more significant due to the b^t factor in the convergence rate. In addition, base $b = 2$ allows for extremely fast implementations using vectorized xor-based arithmetic, which is not the case when $b > 2$. For practical reasons, Sobol' polynomials and initialization matrices have thus been optimized mostly in base $b = 2$ [Joe and Kuo 2008], though consecutive dimensions typically produce increasing t values as dimension increases which limits their use for rendering [Christensen et al. 2018].

Focusing on the case $b = 2$, in this paper we show that there exist many $(1, 2)$-sequences that can be constructed from pairs of irreducible polynomials p and $p^2 + p + 1$. These 2D sequences can be combined to produce higher dimensional (t, s)-sequences of high-quality $t = 1$ in consecutive 2D projections, which is the best quality achievable for $b = 2$ aside from the single $t = 0$ pair mentioned above. We also observed that, in practical integration problems, the quasi-Monte Carlo convergence rate did not differ significantly between $t = 0$ and $t = 1$ in base 2 (see Fig. 3), making $t = 1$ a compelling compromise. Our use of a standard $b = 2$ Sobol' framework makes our sequences readily usable in production renderers already using Sobol' sequences, by simply replacing existing polynomials and initializations with ours. In our quest to prove the quality of our polynomials, we discovered a new recursive construction of Sobol' matrices, derived by iteratively squaring polynomials. This, in turn, led to the identification of interesting patterns that characterize these sequences. This paper explores the depths of this new construction and demonstrates how our sequences can be applied to quasi-Monte Carlo rendering. Code and data are available at https://github.com/liris-origami/OneTwoSobolSequences.

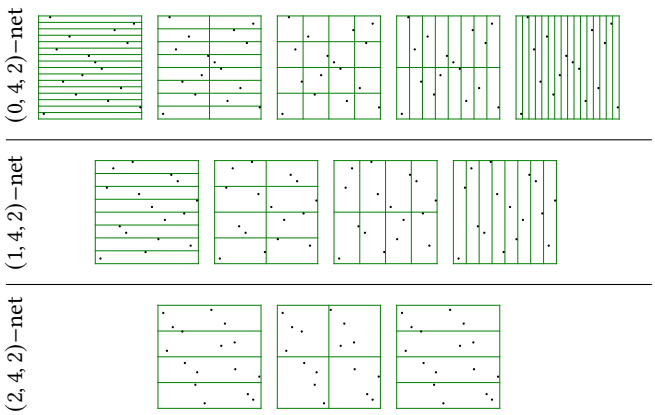


Fig. 2. The definition of a $(t, m, 2)$-net of $n = 2^m$ samples is that all dyadic intervals of area $2^t/2^m$ contain 2^t points. As such, a $(0, 4, 2)$-net (top) has exactly one (=2^0) point in each interval of volume $1/2^4$, a $(1, 4, 2)$-net has exactly two points (=2^1) in each interval of volume $1/2^3$ (middle), and a $(2, 4, 2)$-net has four points on intervals of volume $1/2^2$ (bottom). Increasing t thus reduces uniformity constraints and produces larger gaps and clusters in the distribution.

2 Related work

We summarize fundamentals about Sobol' construction [Sobol' 1967] and refer the reader to reference books [Dick and Pillichshammer 2010; Lemieux 2009; Niederreiter 1992] for in-depth discussions.

Sobol' construction. To construct (t, s)-sequences, Sobol' proposed a solution based on primitive polynomials. Given s primitive polynomials $p_0, \ldots, p_{s-1}$ in the Galois Field of prime base b called $GF(b)$ (think of it as the set of integers modulo b), Sobol' constructs s upper

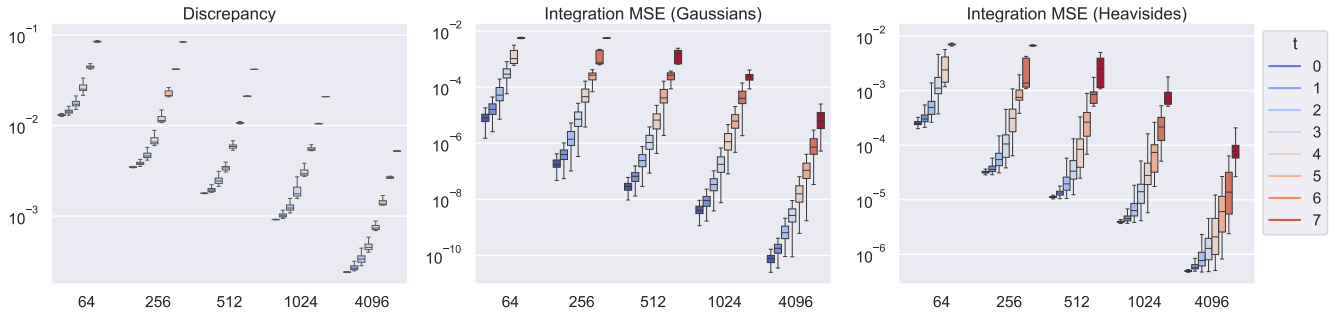


Fig. 3. Experimental validation in 2D of the impact of the t value of a Sobol' sequence on various metrics (from left to right, the generalized L_2 discrepancy [Hickernell 1998] and Monte Carlo integration errors on random Gaussians and Heaviside functions). We randomly select a pair of Sobol' polynomials from the first thousand entries of Joe and Kuo [2008], we evaluate the metrics for each sample count and plot error distribution (box plots) per values t (box plot colors) observed for that sample count (64 realizations for each t). We observe a strong correlation between the observed t value of the point set and its quality for Monte Carlo integration, while $t = 1$ appears as a good compromise in quality compared to $t = 0$.

triangular matrices $M_{p_0}, \ldots, M_{p_{s-1}}$, one per dimension, which are used to obtain each coordinate of the i^{th} sample point $\mathbf{x}_i$ in the sequence. Specifically, the k^{th} coordinate of the i^{th} sample point, $\mathbf{x}_i^k$, is obtained using a matrix-vector product between matrix M_{p_k} and the base b decomposition of the sample point index i interpreted as a column vector, denoted $\bar{i}$ hereafter, $\bar{q} = M_{p_k}\bar{i}$ with $i = \sum_j \bar{i}_j b^j$. The sample point coordinate is now

$$\mathbf{x}_i^k = \sum_j \bar{q}_j b^{-j}\,.$$

The construction of the upper triangular invertible matrix M_{p_k} using the primitive polynomial p_k uses a recursive formula to obtain a column given its e previous columns, where e is the degree of the polynomial p_k. The initialization of this recursion, an $e \times e$ upper triangular matrix at the top-left corner of matrix M_{p_k}, provides additional degrees of freedom in addition to the chosen polynomial. We base our construction on matrix blocks instead of the more common column-wise recursion, as proposed by Faure and Lemieux [2016], that we briefly describe in Sec. 4.1.

Joe and Kuo numerically optimized top-left $e \times e$ blocks, resulting in improved Sobol' sequences on consecutive projections [Joe and Kuo 2008]. Matrices can be directly obtained without Sobol' recurrence using an integer linear program solver, but this limits their use to only moderately large problem [Paulin et al. 2022a].

Faure and Lemieux showed that the larger set of irreducible polynomials can be used instead of primitive polynomials [Faure and Lemieux 2016; Sloane 2001]. Irreducible polynomials are similar to prime numbers, meaning they cannot be factored into products of other non-constant polynomials. Faure and Lemieux showed that the parameter t of the resulting (t, s)-sequence is bounded by the sum of the polynomial degrees minus one. A simple way to obtain $(0, b)$-sequences in base b consists of using the first b irreducible polynomials $p_0(x) = x$, $p_1(x) = x + 1$, $\ldots$, $p_{b-1}(x) = x + b - 1$, each of degree 1. The theorem by Faure and Lemieux then shows that $0 \leq t \leq \sum_i (deg(p_i) - 1) = 0$. However, this produces a unique sequence (up to sample permutations), related to those produced by Faure [1982], which limits its use in more general settings that require sample diversity. Ostromoukhov et al. [2024] used a construction with quadruplets of irreducible polynomials in base $b = 3$ to achieve progressive point sets of excellent consecutive projections.

LDS and projective LDS in Computer Graphics. In rendering applications, low-discrepancy sequences can have a significant impact on path-tracing performance [Christensen et al. 2018; Jarosz et al. 2019; Keller 2004, 2013]. When the sampling pattern defined on the canonical domain $[0, 1)^s$ is mapped to a pixel (or a group of pixels), decorrelating the pattern across different pixels typically requires a scrambling procedure. Owen's scrambling is usually considered, as it preserves the t value of the point set [Owen 1995]. Due to the nature of the rendering equation, several authors have explored projective strategies aimed at achieving highly uniform consecutive 2D projections. Achieving high-quality in 2D projections often comes at the cost of degrading uniformity in higher dimensions [Ahmed and Wonka 2020; Kollig and Keller 2002; Paulin et al. 2021; Perrier et al. 2018]. Notably, the ZeroTwo sequence uses the first two Sobol' dimensions repeatedly with random permutations [Pharr et al. 2023], while padded 4D Sobol' repeats and shuffles samples of the first four dimensions [Burley 2020]. These provide ideal behavior in consecutive 2 or 4D projections, but behave similarly to white noise in higher dimensions. Some methods are dedicated to generating point sets rather than sequences [Ostromoukhov et al. 2024; Paulin et al. 2022a], or are not low discrepancy [Paulin et al. 2020; Reinert et al. 2016]. Our new construction enables the definition of complete $(t, s)-$sequences with guaranteed high-quality (*i.e.* $(1, 2)$-sequences) 2D projections.

3 Overview of our construction

We first focus on 2-dimensional Sobol' sequences. Our goal is thus to obtain Sobol' matrices M_{p_0} and M_{p_1} for two polynomials p_0 and p_1. In our framework, we may use standard Sobol' construction to generate these matrices using respectively polynomials p_0 and p_1 and initialization matrices D_{p_0} and D_{p_1}: our contribution is to provide simple conditions for these initialization matrices to yield high-quality parameter $t = 1$ Sobol' sequences (see Fig. 4). This

section describes an overview of this process, while Sec. 4 details proofs. In the following, we assume modulo 2 arithmetic, and all values involved are binary.

We consider a matrix $K = M_{p_1} M_{p_0}^{-1}$ that uniquely represents a 2D Sobol' sequence up to a permutation of points, called characteristic matrix (denoted C by Ahmed et al. [2023]). We show that when $p_1 = p_0^2 + p_0 + 1$, where p_0 is a degree e polynomial and p_1 thus has degree $2e$, K has a peculiar form, and can be obtained recursively from a decomposition into square blocks A, B and C:

$$K^{(i)} = \begin{bmatrix} A & B \\ 0 & C \end{bmatrix} \rightarrow K^{(i+1)} = \left[\begin{array}{cc|cc} A & B & A+B & A \\ 0 & C & C & 0 \\ \hline 0 & 0 & A & A+B \\ 0 & 0 & 0 & C \end{array}\right].$$

where each block A, B or C has size $2^{i-1}e$. This produces a matrix K of arbitrary size, doubling its size at each iteration. Our paper introduces conditions on $K^{(1)}$ and $K^{(2)}$, that lead to conditions on the Sobol' initialization matrices D_{p_0} and D_{p_1}, for our Sobol' sequences to be $(1,2)$-sequences. We note that the initialization $K^{(1)}$, of size $2e \times 2e$, is $K^{(1)} = D_{p_1} \widetilde{D}_{p_0}^{-1}$, where we denote $\widetilde{D}_{p_0}$ the $2e \times 2e$ matrix obtained by extending the $e \times e$ matrix D_{p_0} to $2e \times 2e$ using standard Sobol' iterations.

To obtain Sobol' initialization matrices, we thus first generate a random invertible triangular $e \times e$ matrix D_{p_0} which we extend to $2e \times 2e$ using Sobol' iterations. We then use a matrix $K^{(1)}$ satisfying our conditions (see next), and easily obtain $2e \times 2e$ initialization matrix $D_{p_1} = K^{(1)} \widetilde{D}_{p_0}$. Matrices M_{p_0} and M_{p_1}, and 2D sample coordinates are then obtained using standard Sobol' procedures, from p_0, $p_1 = p_0^2 + p_0 + 1$, D_{p_0} and D_{p_1}.

To generate higher-dimensional Sobol' sequences, we combine pairs of dimensions but further require that p_0 and $p_1 = p_0^2 + p_0 + 1$ be irreducible polynomials so as to guarantee that the resulting s-dimensional sequence is a (t, s)-sequence [Faure and Lemieux 2016].

We claim the following contributions.

Theorem 3.1. *The sequence of iterations*

$$K^{(i)} = \begin{bmatrix} A & B \\ 0 & C \end{bmatrix} \rightarrow K^{(i+1)} = \left[\begin{array}{cc|cc} A & B & A+B & A \\ 0 & C & C & 0 \\ \hline 0 & 0 & A & A+B \\ 0 & 0 & 0 & C \end{array}\right], \quad (1)$$

where each matrix block A, B, C, is of size $2^{i-1}e \times 2^{i-1}e$, produces the characteristic matrix of a 2D Sobol' sequence given by a degree e polynomial p, and degree $2e$ polynomial $p^2 + p + 1$.

Corollary 3.2. *A 2D Sobol' sequence given by polynomials p and $p^2 + p + 1$ only depends on the degree of the polynomial and initialization matrices, and does not depend on the coefficients of p themselves, up to a permutation of samples.*

This corollary is readily justified since the recursive construction of theorem 3.1 does not involve polynomial coefficients, but merely polynomial degrees. As such, a pair p_0 of degree e and $p_1 = p_0^2 + p_0 + 1$ with given initialization matrices would result in the same sequence as p_0' of degree e and $p_1' = p_0'^2 + p_0' + 1$ for *another pair* of initialization matrices.

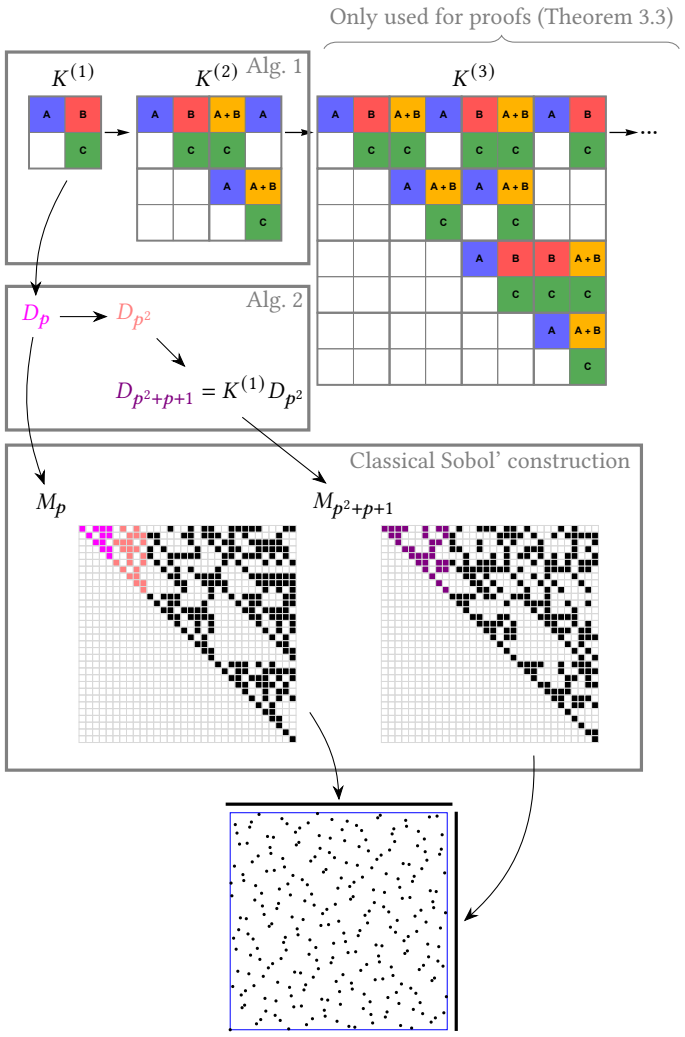


Fig. 4. Overview. We introduce a recursive construction of the characteristic matrix associated with a pair of polynomials $(p, p^2 + p + 1)$. We use it in proofs to obtain conditions for generating $(1, 2)$-sequences based on the first iteration alone of this recursion. From characteristic matrices meeting these conditions, we derive Sobol' initialization matrices D_p and D_{p^2+p+1}, which in turn allows to construct the corresponding Sobol' matrices M_p and M_{p^2+p+1} generating $(1, 2)-$sequences in base 2.

Theorem 3.3. *Iterations $K^{(i)} \rightarrow K^{(i+1)}$ characterize Sobol' $(1, 2)$-sequences if and only if both conditions are met:*

- $(\mathcal{P})$: $\mathrm{corank}(T) \leq 1$ *for any rectangular* $(w-1) \times w$ *submatrix* T *of* $K^{(2)}$ *anchored at its first row*
- $(\mathcal{Q})$: $\mathrm{corank}(C') \leq 1$ *for any square submatrix* C' *of block* C *in* $K^{(1)}$ *obtained by removing any consecutive set of* k *columns and the last* k *rows of* C.

These results allow us to pre-compute many matrices $K^{(1)}$ satisfying the conditions of theorem 3.1 for a given polynomial degree e

and infer pairs of irreducible polynomials and initialization matrices that produce Sobol' $(1,2)$-sequences.

In the process of proving these theorems, we discovered new insights on Sobol' constructions for more general polynomials:

- Polynomials p and p^2 will produce the same Sobol' matrices, given proper initialization matrices (see lemma 4.1).
- This property allows building general Sobol' matrices in a recursive way by doubling their size at each iteration via polynomial squaring.
- The characteristic matrix can also be constructed recursively.

The goal of Sec. 4 is to provide mathematical proofs for the claims we summarized in this overview section. The practitioner may thus skip Sec. 4 at first read and jump to the description of our algorithms in Sec. 5. Specifically, sections 4.1 and 4.2 prove lemma 4.1 related to polynomials p and p^2 yielding the same matrices. This in turns helps proving in Sec. 4.3 that characteristic matrices can be constructed recursively. When applied to polynomials p and p^2+p+1, Sec. 4.4 proves that the characteristic matrix has the recursive construction of Eq. 1 and thus proves Theorem 3.1. Finally, Sec. 4.5 and our supplementary materials prove Theorem 3.3 that explicits conditions under which the characteristic matrices generate $(1,2)$-sequences.

4 Construction of $(1,2)$-sequences in base 2

We first recall a construction of Sobol' matrices based on matrix blocks by Faure and Lemieux [2016] in Sec. 4.1, which will serve as a basis for the next sections describing our proof. Our proof first consists of introducing a new recursive construction of Sobol' matrices by squaring polynomials in Sec. 4.2. We then show that a similar squaring procedure can be obtained for characteristic matrices in Sec. 4.3. We then show, using this construction, that the characteristic matrix for polynomials p and p^2+p+1 has a specific form exhibiting a self-similar pattern in Sec. 4.4. We finally show that ranks of characteristic matrices with this self-similar pattern are necessarily such that the produced 2D sequences are $(1,2)$-sequences in Sec. 4.5.

4.1 Block-based recursive construction

We first briefly describe a block-based 1-D Sobol' construction as described by Faure and Lemieux [2016].

For a given irreducible polynomial $p(x) = x^e + \sum_{i=0}^{e-1} a_i x^i$ and upper $e \times e$ invertible triangular initialization matrix D_p, Faure and Lemieux [2016] rewrite Sobol' iterations in terms of block matrices:

$$M_p = \begin{pmatrix} B_{1,1} & B_{1,2} & B_{1,3} & \dots \\ 0 & B_{2,2} & B_{2,3} & \dots \\ 0 & 0 & B_{3,3} & \dots \\ \vdots & \vdots & \vdots & \ddots \end{pmatrix},$$

where the blocks $B_{i,j}$, of size $e \times e$, are defined according to the following recursive procedure:

$$B_{1,1} = D_p; \quad B_{i,i} = D_p F_p^{i-1}$$

$$B_{i,j} = \begin{cases} B_{i,j-1} Q_p F_p & \text{when } i = 1 \\ B_{i,j-1} Q_p F_p + B_{i-1,j-1} F_p & \text{elsewhere.} \end{cases} \tag{2}$$

Here, Q_p is an $e \times e$ lower triangular Toeplitz matrix involving the coefficients $(a_i)_i$ of polynomial p:

$$Q_p = \begin{pmatrix} a_0 & 0 & 0 & \dots & 0 \\ a_1 & a_0 & 0 & \dots & 0 \\ a_2 & a_1 & a_0 & \dots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ a_{e-1} & a_{e-2} & a_{e-3} & \dots & a_0 \end{pmatrix}. \tag{3}$$

Matrix F_p of size $e \times e$ is defined as

$$F_p = (Id_e + R_{p,2})(Id_e + R_{p,3}) \dots (Id_e + R_{p,e}), \tag{4}$$

where Id_e is an identity matrix of size $e \times e$, and $R_{p,k}$ are matrices of size $e \times e$ with zeros everywhere except in the first $k-1$ entries of the k-th column, given by the coefficients $(a_{e-(k-1)}, \dots, a_{e-1})$ of polynomial p.

We introduce a new recursion to build Sobol' matrices inspired by the construction of Faure and Lemieux [2016].

4.2 Sobol' construction by squaring polynomials

In the following, we introduce a squared superscript notation to clarify matrix sizes when appropriate, e.g., $M_p^{[2e]}$ denoting the Sobol' matrix of polynomial p restricted to the first $2e$ rows and $2e$ columns.

We observe that the Sobol' matrix M_{p^2} of a squared polynomial (although not irreducible) is identical to the Sobol' matrix M_p of the original polynomial, provided that the initialization matrix D_{p^2} coincides with the top-left corner of M_p. We formalize this:

Lemma 4.1. *The Sobol' matrix M_p generated by a polynomial p of degree e and initialization matrix D_p is identical to the Sobol' matrix M_{p^2} of polynomial p^2 and initialization matrix*

$$D_{p^2} = M_p^{[2e]} = \begin{pmatrix} D_p & 0 \\ 0 & D_p \end{pmatrix} \begin{pmatrix} Id_e & Q_p F_p \\ 0 & F_p \end{pmatrix}, \tag{5}$$

corresponding to the top-left $2e \times 2e$ submatrix of M_p.

Matrices Q_{p^2} and F_{p^2} of Faure and Lemieux [2016] can be obtained by applying a Kronecker product (or tensor product) with the matrix $Id_2 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ to matrices Q_p and F_p:

$$Q_{p^2} = Q_p \otimes Id_2, \qquad F_{p^2} = F_p \otimes Id_2. \tag{6}$$

where Q_{p^2} and F_{p^2} are of size $2e \times 2e$.

This lemma brings a new recursive construction of Sobol' matrices, doubling their sizes at each iteration by squaring polynomials, illustrated in Fig. 5.

In our development, we first note that, while F_p can have a complicated form, its inverse can be expressed much more easily, as an upper triangular Toeplitz matrix:

$$F_p^{-1} = \begin{pmatrix} 1 & a_{e-1} & a_{e-2} & \dots & a_1 \\ 0 & 1 & a_{e-1} & \dots & a_2 \\ 0 & 0 & 1 & \dots & a_3 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \dots & 1 \end{pmatrix}, \tag{7}$$

where we ignore signs in modulo 2 arithmetic. This is obtained by observing that matrices $Id_e + R_{p,k}$ are their own inverses, and that

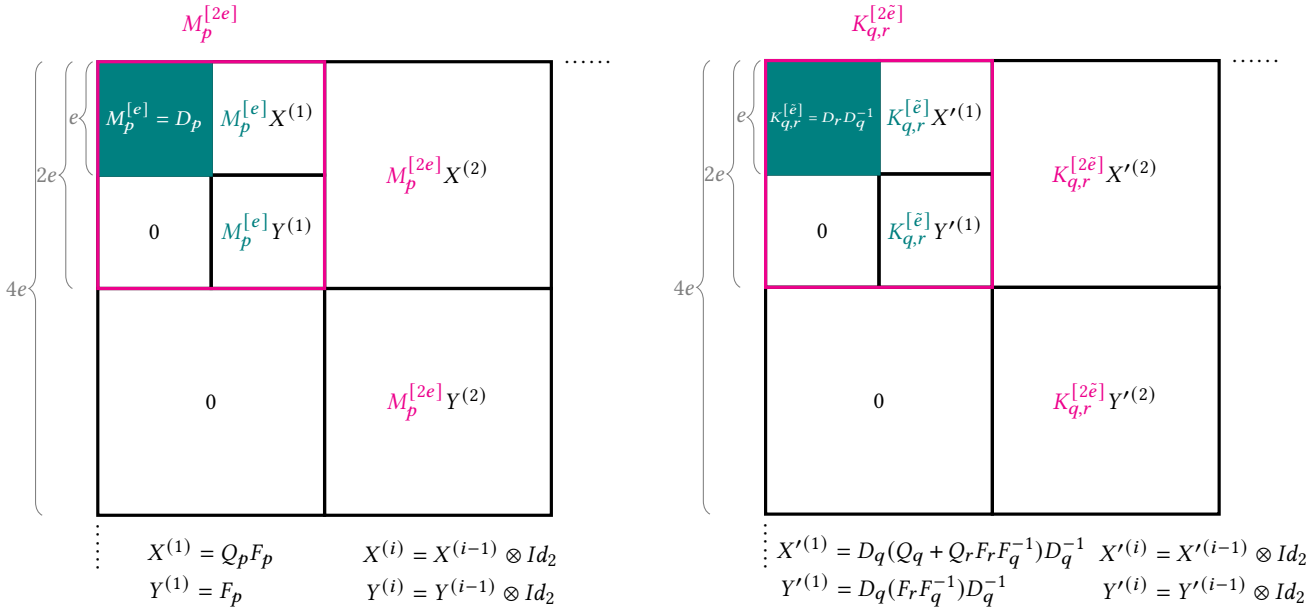


Fig. 5. In contrast to the column-by-column Sobol' approach [Sobol' 1967], and the block formulation of Faure and Lemieux [2016] (Sec. 4.1), we present a novel recursive construction for Sobol' matrices (left) and characteristic matrices (right) by squaring polynomials. The construction of matrix M_p follows from lemma 4.1, Eq. (5), while the construction of $K_{q,r}^{[2\tilde{e}]}$ is obtained from Eq. (8). Matrices $X^{(i)}$, $Y^{(i)}$, $X'^{(i)}$ and $Y'^{(i)}$ provide compact representations of expressions involving D_p, F_p, and Q_p, using the distributivity of the Kronecker product over matrix multiplication.

inverting F_p then merely reverses the order of the multiplication: $F_p^{-1} = (Id_e + R_{p,e}) \dots (Id_e + R_{p,2})$.

Proof of Lemma 4.1. The relation between D_{p^2} and D_p is simply obtained by running Faure and Lemieux' iterations for one block of columns. We may now assume that the top-left $2e \times 2e$ submatrices of M_p and M_{p^2} coincide. We also note that for a polynomial $p(x) = x^e + \sum_{i=0}^{e-1} a_i x^i$, given modulo-2 arithmetic cancelling odd degrees, $p^2(x) = x^{2e} + \sum_{i=0}^{e-1} a_i x^{2i}$. This, in turn, leads to $Q_{p^2} = Q_p \otimes Id_2$, and similarly, to $F_{p^2}^{-1} = F_p^{-1} \otimes Id_2$ and thus $F_{p^2} = F_p \otimes Id_2$ (the inverse of the Kronecker product being the Kronecker product of the inverse matrices), and finally, $Q_{p^2} F_{p^2} = (Q_p F_p) \otimes Id_2$. The recursive construction of Eq. (2) thus produces the same matrices whether using Q_{p^2} and F_{p^2} or Q_p and F_p. □

4.3 Block-based characteristic matrices

For a pair of dimensions with Sobol' matrices M_q and M_r, we base our analysis on the characteristic matrix $K = M_r M_q^{-1}$ as defined by Ahmed et al. [2023] , which uniquely characterizes Sobol' 2D sequences up to a permutation of samples. When the polynomials q and r are of the same degree $\tilde{e}$, we may build a characteristic matrix of size $2\tilde{e}$ by applying one iteration of Faure and Lemieux' block construction:

$$
\begin{aligned}
K_{q,r}^{[2\tilde{e}]} &= M_r^{[2e]} \left(M_q^{[2e]}\right)^{-1} \\
&= \begin{pmatrix} D_r & 0 \\ 0 & D_r \end{pmatrix} \begin{pmatrix} Id_{\tilde{e}} & Q_r F_r \\ 0 & F_r \end{pmatrix} \left(\begin{pmatrix} D_q & 0 \\ 0 & D_q \end{pmatrix} \begin{pmatrix} Id_{\tilde{e}} & Q_q F_q \\ 0 & F_q \end{pmatrix} \right)^{-1} \\
&= \begin{pmatrix} D_r & 0 \\ 0 & D_r \end{pmatrix} \begin{pmatrix} Id_{\tilde{e}} & Q_q + Q_r F_r F_q^{-1} \\ 0 & F_r F_q^{-1} \end{pmatrix} \begin{pmatrix} D_q & 0 \\ 0 & D_q \end{pmatrix}^{-1} \\
&= \begin{pmatrix} K_{q,r}^{[\tilde{e}]} & 0 \\ 0 & K_{q,r}^{[\tilde{e}]} \end{pmatrix} \begin{pmatrix} Id_{\tilde{e}} & D_q(Q_q + Q_r F_r F_q^{-1}) D_q^{-1} \\ 0 & D_q(F_r F_q^{-1}) D_q^{-1} \end{pmatrix}. \qquad (8)
\end{aligned}
$$

where we used the identity $\begin{pmatrix} A & B \\ 0 & C \end{pmatrix}^{-1} = \begin{pmatrix} A^{-1} & -A^{-1}BC^{-1} \\ 0 & C^{-1} \end{pmatrix}$ for invertible A and C, and where $K_{q,r}^{[\tilde{e}]} = D_r D_q^{-1}$ is the $\tilde{e} \times \tilde{e}$ initialization block for this characteristic matrix, obtained from the initializations of M_q and M_r.

This construction considers polynomials q and r of the same degree, but we can use lemma 4.1 to square our first polynomial and then consider $q = p^2$ and $r = p^2 + p + 1$ of the same degree. We thus consider this construction using $\tilde{e} = 2e$.

Also, this construction merely produces a matrix of size $2\tilde{e}$ given polynomials of degree $\tilde{e}$. However, it can be used recursively by considering lemma 4.1, doubling the size of the matrix at each iteration by squaring polynomials. By lemma 4.1, the effect of squaring polynomials on all matrices involved is merely a tensor product with Id_2. We also illustrate this process in Fig. 5.

4.4 The special case (p, p^2+p+1)

The construction for characteristic matrices in Sec. 4.3 is general, and applies to any pair of polynomials. In this section, we show the special case when $q = p^2$, and $r = p^2+p+1$.

First, we note that applying lemma 4.1 for using $q = p^2$ in place of $q = p$ leads to an extended initialization matrix D_{p^2} which inverse can be expressed:

$$D_{p^2}^{-1} = \left(M_p^{[2e]}\right)^{-1} = \begin{pmatrix} Id_e & Q_p \\ 0 & F_p^{-1} \end{pmatrix} \begin{pmatrix} D_p^{-1} & 0 \\ 0 & D_p^{-1} \end{pmatrix}. \tag{9}$$

We thus now consider that our polynomials have degree $2e$ and we seek to apply our characteristic matrix construction to obtain a matrix $K_{q,r}^{[4e]}$ of size $4e \times 4e$.

It can then be shown (see Appendix A.1) that $F_{p^2+p+1}F_{p^2}^{-1}$ has a particular form:

$$F_{p^2+p+1}F_{p^2}^{-1} = \begin{pmatrix} Id_e & F_p \\ 0 & Id_e \end{pmatrix}. \tag{10}$$

The resulting matrix is also its own inverse: $F_{p^2+p+1}F_{p^2}^{-1} = F_{p^2}F_{p^2+p+1}^{-1}$. Combining Eq. (9) and (10) (see Appendix A.2), we have:

$$F_{p^2+p+1}F_{p^2}^{-1}D_{p^2}^{-1} = D_{p^2}^{-1}\begin{pmatrix} Id_e & Id_e \\ 0 & Id_e \end{pmatrix}. \tag{11}$$

Similarly, we have

$$(Q_{p^2} + Q_{p^2+p+1}F_{p^2+p+1}F_{p^2}^{-1})D_{p^2}^{-1} = D_{p^2}^{-1}\begin{pmatrix} Id_e & Id_e \\ Id_e & 0 \end{pmatrix}, \tag{12}$$

where we further use the properties of the product of our Toeplitz matrices, see Appendix A.3 for details.

Putting all together, and considering the initially given matrix $K_{p^2,p^2+p+1}^{[2e]}$ has size $2e$ since we considered p^2 and p^2+p+1 of degree $2e$, we see that the recursive construction of K becomes

$$K_{p^2,p^2+p+1}^{[4e]} = \begin{pmatrix} K_{p^2,p^2+p+1}^{[2e]} & 0 \\ 0 & K_{p^2,p^2+p+1}^{[2e]} \end{pmatrix} \begin{pmatrix} Id_{2e} & \begin{pmatrix} Id_e & Id_e \\ Id_e & 0 \end{pmatrix} \\ 0 & \begin{pmatrix} Id_e & Id_e \\ 0 & Id_e \end{pmatrix} \end{pmatrix}. \tag{13}$$

Lemma 4.1 indicates that this procedure becomes recursive by squaring polynomials, allowing to double the size of K at each iteration. We rewrite these iterations using the following notation involving blocks A, B, C of size $2^i e \times 2^i e$, doubling their size at each iteration:

$$K^{(i)} = \left[\begin{array}{cc} A & B \\ 0 & C \end{array}\right] \rightarrow K^{(i+1)} = \left[\begin{array}{cc|cc} A & B & A+B & A \\ & C & C & 0 \\ \hline & & A & A+B \\ & & & C \end{array}\right]$$

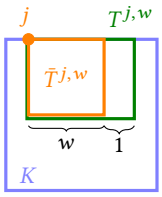
with the $2e \times 2e$ initial matrix

$$\begin{aligned} K^{(1)} &= K_{p^2,p^2+p+1}^{[2e]} = D_{p^2+p+1}D_{p^2}^{-1} \\ &= D_{p^2+p+1}\left(\begin{pmatrix} D_p & 0 \\ 0 & D_p \end{pmatrix}\begin{pmatrix} Id_e & Q_pF_p \\ 0 & F_p \end{pmatrix}\right)^{-1}, \end{aligned}$$

for any given $e \times e$ upper triangular invertible matrix D_p and $2e \times 2e$ upper triangular invertible matrix D_{p^2+p+1} giving the degrees of freedom for the generated sequences. D_{p^2} is here obtained by running standard Sobol' iterations to extend the $e \times e$ matrix D_p to obtain the next e rows and columns.

4.5 Rank of submatrices

Let us denote by $\bar{T}^{j,w}$ a square $w \times w$ submatrix of K starting at column $1 \leq j < m - w$. Ahmed et al. [2023] showed that (M_p, M_q) is a $(0,2)-$sequence if and only if all submatrices $\bar{T}^{j,w}$ have nonzero determinant (modulo 2). In our settings, we define $T^{j,w}$ as the rectangular submatrix of K starting at column j and of size $(w-1) \times w$. A first claim is that a $(1,2)$-sequence is characterized by a matrix K having all submatrices $T^{j,w}$ rank-deficient by at most 1 (see Appendix A.4). If we denote $\text{corank}(T^{j,w}) := w - 1 - \text{rank}(T^{j,w})$ the rank deficiency of matrix $T^{j,w}$, a $(1,2)$-sequence is thus characterized by the property that all submatrices $T^{j,w}$ of K have a corank of at most 1. We call this property $\mathcal{P}$. Ranks need to be computed in $GF(2)$, e.g., the matrix $\begin{bmatrix} 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 1 \\ 0 & 1 & 1 & 1 \end{bmatrix}$ has rank 2 in $GF(2)$ (because the third column is the sum of the previous two, modulo 2) although it has rank 3 over the integers. This can be obtained numerically using Gaussian elimination.



Since matrix K is an infinite-sized matrix, systematic numerical evaluation of ranks for all possible submatrices of K quickly becomes intractable.

We instead benefit from our recursive construction of K to propagate properties across iterations. We show by induction that if property $\mathcal{P}$ holds for matrix $K^{(2)}$, and an additional property $\mathcal{Q}$ holds for the block C of $K^{(1)}$, then properties $\mathcal{P}$ and $\mathcal{Q}$ necessarily hold for all $K^{(i)}$, $i \geq 1$.

Property $\mathcal{Q}$ states that all submatrices C' of C obtained by removing $1 \leq t < m$ consecutive columns and the last t rows have $\text{corank}(C') \leq 1$. It is easy to verify that property $\mathcal{Q}$ holds for $K^{(i)}$, $i \geq 1$, if it holds for $K^{(1)}$, since the recursive procedure transforms C into a block triangular matrix $\begin{pmatrix} A & A+B \\ 0 & C \end{pmatrix}$, where A is full rank.

Verifying by induction that property $\mathcal{P}$ holds for $K^{(i)}$, $i \geq 1$, provided that it holds for $K^{(2)}$ (and thus $K^{(1)}$) is more involved. Given a matrix of the form $K^{(i)}$, we iterate our construction to obtain $K^{(i+1)}$ and $K^{(i+2)}$; $K^{(i+2)}$ has 8×8 blocks, each of size $2^{i-1}e \times 2^{i-1}e$. From $K^{(i+2)}$, we extract matrices $T^{j,w}$ that overlap any number $1 \leq b \leq 8$ of consecutive blocks horizontally and either b or $b-1$ blocks vertically. We symbolically perform Gaussian elimination on $T^{j,w}$ to exhibit block triangular structures for which ranks can be easily obtained [Meyer 1973]. Specifically, we seek to have any number of blocks on the diagonal with full rank, and, at most, 1 block fulfilling property $\mathcal{P}$ or $\mathcal{Q}$ by hypothesis to conclude that $\text{corank}(T^{j,w}) \leq 1$. Given the sheer number of cases, we refer the reader to the supplementary materials for the exhaustive list of cases, and show one typical case in Fig. 6 on a submatrix $T = T^{j,w}$ overlapping 4 blocks (out of 8) of $K^{(i+2)}$. The base case of the

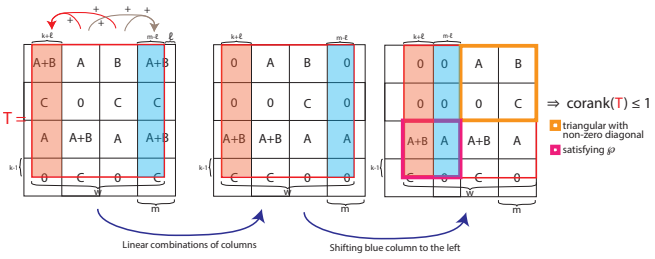


Fig. 6. Example of an $(s-1)\times s$ submatrix T (in red) of $K^{(i+2)}$ overlapping 4 consecutive blocks horizontally and vertically. Gaussian elimination is performed (here by addition and permutation of blocks of columns) to exhibit a block triangular structure, where one block (in orange) has non-zero determinant, and another block (in pink) whose corank is smaller than 1 since $K^{(i+1)}$ satisfies $\mathcal{P}$ by hypothesis. This proves that this particular submatrix T also has corank$(T) \leq 1$. In supplementary materials, we exhaustively list all cases for rectangular submatrices T included in $K^{(i+2)}$ to conclude that $K^{(i+2)}$ then satisfies $\mathcal{P}$.

induction is tested numerically on matrix $K^{(2)}$ (if it holds for $K^{(2)}$ it also holds for $K^{(1)}$).

5 Experimental results

In this section, we outline practical aspects of our method. First, we provide a brief overview of the process for generating polynomials and initialization matrices for Sobol' sequences, with a focus on ensuring high-quality 2D projections. Next, we present a concrete example demonstrating how the proposed method can be integrated into a typical physically-based rendering (PBR) framework, using PBRT [Pharr et al. 2023] as a case study.

5.1 Constructing projective $(1,2)$-sequences

In our construction, we cannot use all irreducible polynomials as Faure and Lemieux do [Faure and Lemieux 2016], because we focus on pairs of polynomials (p_i, p_{i+1}) such that $p_{i+1} = p_i^2 + p_i + 1$. We found 346 such pairs of irreducible polynomials of degree up to $e = 16$ ($2e = 32$). This allows for 692D sampling with guaranteed-quality 2D projections, and more precisely $(1,2)$-sequences for consecutive pairs of dimensions. The property of $(1,2)$-sequences for each pair is guaranteed by Theorem 3.1, provided that the appropriate initialization matrices are provided.

First, we precompute a set of candidate characteristic matrices $\mathcal{K}_e$ for each degree e of the polynomials we are considering. Note that by Corollary 3.2, at this stage we do not need the specific polynomials involved, but only their degrees. The construction of this collection consists in a random search for matrices A, B, C of size $e \times e$ by verifying that $K^{(2)}$ satisfies property $\mathcal{P}$ and that C satisfies property $\mathcal{Q}$ (see Sec. 4.5 and Algorithm 1). Exploring the space of all matrices A, B, C that satisfy $\mathcal{P}$ and $\mathcal{Q}$, respectively, becomes infeasible for large e, as the search space grows exponentially with e. For $e \in \{1,2,3,4,5\}$, we found 2, 6, 40, 1688, and 727 matrices, respectively. For higher degrees, we leverage the fact that doubling a matrix in $\mathcal{K}_e$ by squaring the polynomial as described in Eq. (1), provides a candidate matrix for $\mathcal{K}_{2e}$. These matrices are available in the supplementary material.

ALGORITHM 1: Constructing $\mathcal{K}_e$.

Result: A set of candidate characteristic matrices $\mathcal{K}_e$.
while *true* **do**
  Draw a random upper triangular matrix A with 1 on the diagonal and a random square matrix B, both of size $e \times e$;
  Draw a random triangular matrix C of size $e \times e$ satisfying the property $\mathcal{Q}$;
  Construct $K^{(2)}$ of size $4e \times 4e$ using Eq. (1);
  if $K^{(2)}$ *satisfies the property* $\mathcal{P}$ **then**
    Append $K^{(1)}$ to $\mathcal{K}_e$;
  end
end

Then, each characteristic matrix in $\mathcal{K}_e$ is used to define two Sobol' matrices for each pair of irreducible polynomials (p, p^2+p+1) of degrees e and $2e$ respectively (Theorem 3.1). We construct the initialization matrices $D_p^{[e]}$ and $D_{p^2+p+1}^{[2e]}$ as follows: we draw a random non-singular upper triangular matrix $D_p^{[e]}$ of size $e \times e$, and expand it to $D_{p^2}^{[2e]}$ using standard Sobol' iterations for polynomial p, and construct $D_{p^2+p+1}^{[2e]}$ using $D_{p^2+p+1}^{[2e]} = K^{[2e]} D_{p^2}^{[2e]}$ where the characteristic matrix $K^{[2e]}$ is drawn from $\mathcal{K}_e$ (see Algorithm 2).

Finally, we convert the initialization matrices $D_p^{[e]}$ and $D_{p^2+p+1}^{[2e]}$ into a set of direction vectors for Sobol' construction, which is compatible with the format of Joe and Kuo [2008].

ALGORITHM 2: Constructing many $(1,2)-$sequence initialization matrices

Data: a degree e, a set of candidate characteristic matrices $\mathcal{K}_e$.
Result: A collection of tuples $\left\{\left(p, D_p^{[e]} \text{and} D_{p^2+p+1}^{[2e]}\right)\right\}$
while *true* **do**
  forall *pairs of irreducible polynomials* p *and* p^2+p+1 *of degrees* e *and* $2e$ *respectively* **do**
    Create random non-singular upper triangular matrix $D_p^{[e]}$ of size $e \times e$;
    Expand $D_p^{[e]}$ to $D_{p^2}^{[2e]}$ using Sobol' construction with p;
    Draw a characteristic matrix $K^{[2e]}$ from $\mathcal{K}_e$;
    Compute $D_{p^2+p+1}^{[2e]} = K^{[2e]} D_{p^2}^{[2e]}$;
    Append $\left(p, D_p^{[e]}, D_{p^2+p+1}^{[2e]}\right)$ to the result;
  end
end

5.2 Further improvements

For each pair of polynomials (p_i, p_{i+1}) we can generate a large number of possible initializations, as outlined in Algorithm 2, which all satisfy our conditions for generating $(1,2)$-sequences. Consequently, we enforce additional criteria to enhance our multi-dimensional construction. In the context of computer graphics, we aim to achieve higher quality not only for consecutive pairs of dimensions but also for 4-tuples of dimensions, which group consecutive pairs. We select only solutions with guaranteed reasonably-good $t \leq 4$ for 4D

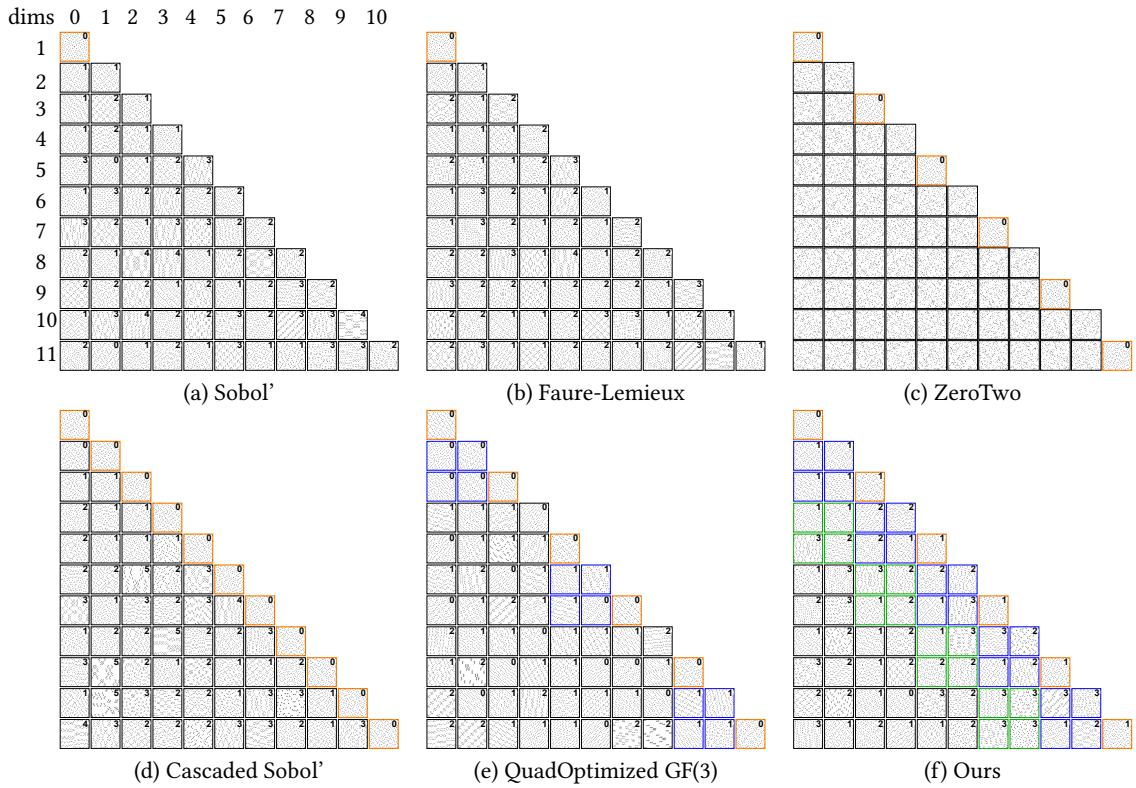


Fig. 7. We compare consecutive 2D projections for the first 12 dimensions of several constructions: (a) Sobol' with Joe and Kuo initializations [Joe and Kuo 2008], (b) Faure and Lemieux [2016; 2019], (c) the first two Sobol' dimensions, repeated with a random permutation of sample indices [Pharr et al. 2023], (d) the Cascaded Sobol' approach of Paulin et al. [2021] (not sequence) (e) the Quad-optimized LDS in GF(3) by Ostromoukhov et al. [2024], and (f) our approach. Here, orange squares designate guaranteed $(0,2)$-progressive or $(0,2)/(1,2)$-sequence properties. Blue squares designate optimized 4-tuples of dimensions. Green squares designate additional optimizations, supported by our optimization process (See details in Sec. 5.2). For low discrepancy projections, the factor t of each point set is numerically computed and indicated in the upper-right corner of each patch.

projections up to 2^{15} points. We further seek to achieve low t for dimensions that are close to $(i, i+1)$. Specifically, pairs of dimensions are progressively added by proposing pairs of matrices generated from characteristic matrices. Accepting a new pair of matrices requires that, within the 6D block of dimensions involving the last 4D block and the new pair, all-pairs 2D values of $t \leq 3$ for any $m \leq 8$. Further, for the 4D block involving the last pair of dimensions and the new pair, the 4D value of $t \leq 4$ for $m \leq 15$ and $t \leq 3$ for $m \leq 10$. Pairs of polynomials of degree lower than $e = 12$ (involving the first 36 dimensions) were further inspected manually to ensure high quality. This optimization process is inspired by the pioneering works of Joe and Kuo [2008] and Faure and Lemieux [2019]. It is also close to the optimization described by Ostromoukhov et al. [2024]. Visualization of 2D projections for our resulting sequence can be seen in Fig. 7 while discrepancy and integration errors for 2D and 4D projections can be seen in Fig. 10. In Figure 8, we further analyze the experimental t values any 2D projections, for various sample counts, up to 100D. While our construction provides better t values for nearly consecutive pairs (see histograms), the experimental t values for distant polynomials are only slightly worse than Sobol's.

It is important to note that, aside from the optimization criteria, our construction behaves like any other Sobol' construction. Specifically, some remote pairs of dimensions or n-tuples beyond the optimized 4-tuples mentioned earlier may exhibit "good" or "bad" values of t, which fall outside the control of our optimization process. This limitation is also present in the aforementioned optimizations [Faure and Lemieux 2019; Joe and Kuo 2008; Ostromoukhov et al. 2024].

For dimensions greater than 692, the standard Joe and Kuo initializations can be used, provided they do not reuse our optimized polynomials. To assist with this, we provide a complementary initialization table for reference, along with the corresponding initialization matrices, integrating Joe and Kuo's dimensions for dimensions greater than 692 that excludes our polynomials.

5.3 Renderings

We evaluate our sequence with PBRT-v4 [Pharr et al. 2023] used as a per-pixel path tracer. PBRT constructs paths by combining 1D and 2D random variables. When sampling 1D variables, we sample 2 of our dimensions and keep one of them cached for the next 1D variable. Constructing a path involves sampling a pixel (2D), time (1D) and the lens (2D). Evaluating direct lighting additionally requires selecting the light source (1D) and a point on that light source (2D). Evaluating one bounce of indirect lighting requires

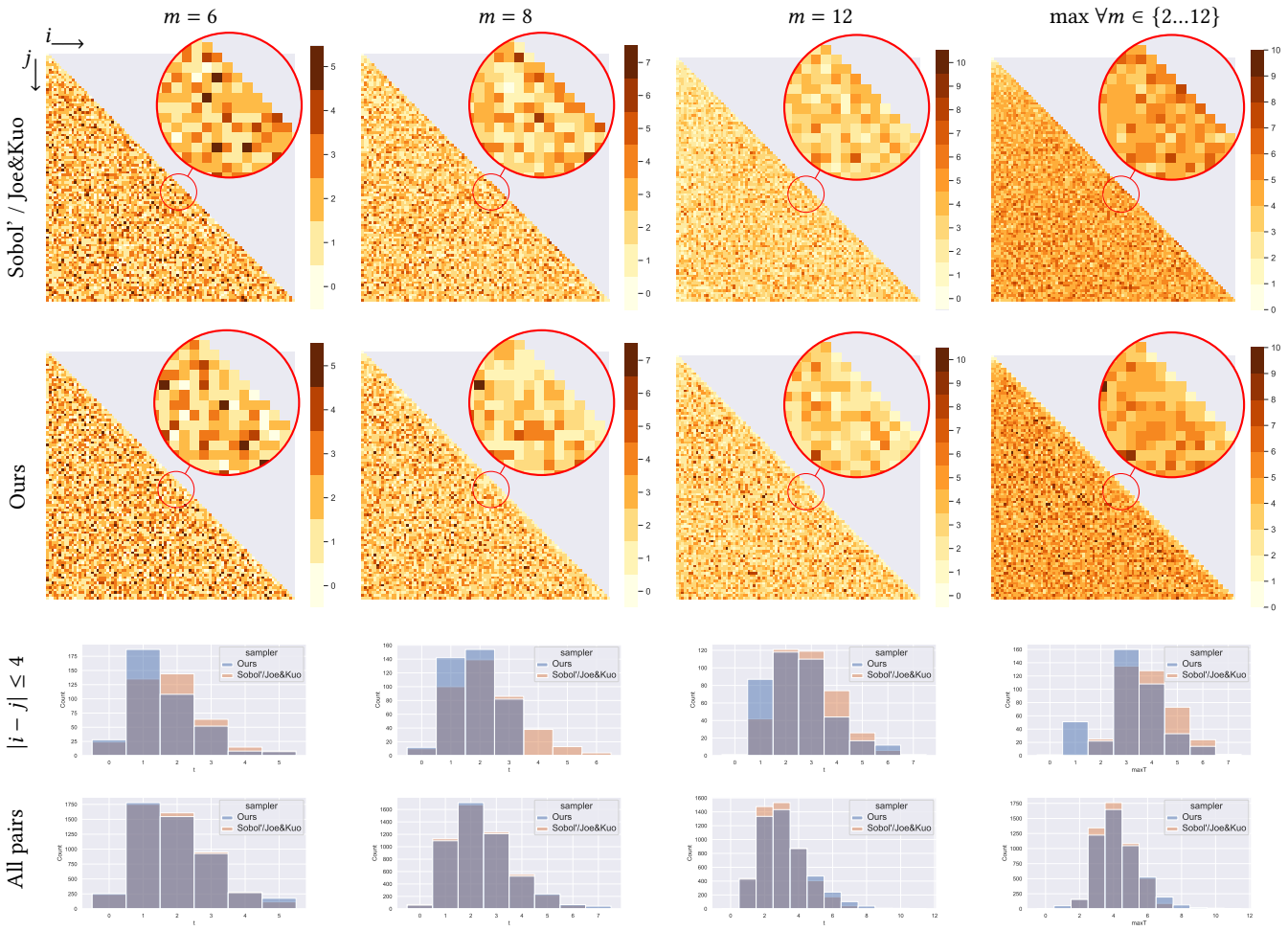


Fig. 8. Up to 100 dimensions, we show the experimental t values for each 2D projection pair (i, j) of Sobol' sequences with Joe and Kuo (top) and our $(1, 2)$-sequences (bottom) for $m = 6$, $m = 8$, and $m = 12$. The last column corresponds to the maximum t values over $m \in \{2, .., 12\}$. The histograms highlight the distributions of t values for close pairs (*i.e.*, $|i - j| \leq 4$) and all pairs. While most pairs have comparable t values with only a small degradation far from the diagonal, our construction shows a significant improvement for close consecutive pairs (with $t \leq 1$ by construction for pairs $(2i, 2i + 1)$).

selecting the material (1D) and sampling a direction from it (2D). In this setting, rendering with direct lighting uses 11 dimensions involving 6 optimized pairs, while rendering with one bounce of indirect lighting requires 17 dimensions (9 pairs), two bounces of indirect lighting require 23 dimensions (12 pairs), etc. We did not use Russian roulette nor spectrum sampling. We compare our results to those of other samplers in Fig. 12, focusing on rendering error. We used Owen scrambling for all methods.

Our sequences with guaranteed $t = 1$ 2D projections perform similarly to the base-3 progressive point sets of quad-optimized $GF(3)$ [Ostromoukhov et al. 2024] and the base-2 point sets of Cascaded Sobol' [Paulin et al. 2021]. This result is in agreement with other discrepancy and integration results in Fig. 10 and Fig. 9. Padding 4D Sobol' samples with random shuffling [Burley 2020] yields better results than padding in 2D (ZeroTwo [Pharr et al. 2023]). While our high-dimensional behavior is guaranteed low-discrepancy and padded 4D Sobol' has poor discrepancy convergence (see Fig. 11), our renderings remain similar in most cases.

Working with $GF(2)$ arithmetic is also faster than $GF(3)$. Additions in $GF(2)$ can be computed with a binary *xor* in parallel on 32 values whereas $GF(3)$ requires modulo arithmetic and tabulated operations on scalar values [Ostromoukhov et al. 2024]. Generating 8D points is roughly four time slower with quad-optimized $GF(3)$ (798ms vs 201ms respectively, for 16M samples, on a Ryzen 3900X). In our tests, when rendering a Cornell box at 256spp at 1k resolution, sampling (in base-2) takes at least 75% of the total render time in PBRT, while the more complex SanMiguel scene results in 15% of the time spent in sampling. Easy-to-use precompiled matrices and fast point generation functions are available in the supplementary materials, as well as the modified PBRT source code.

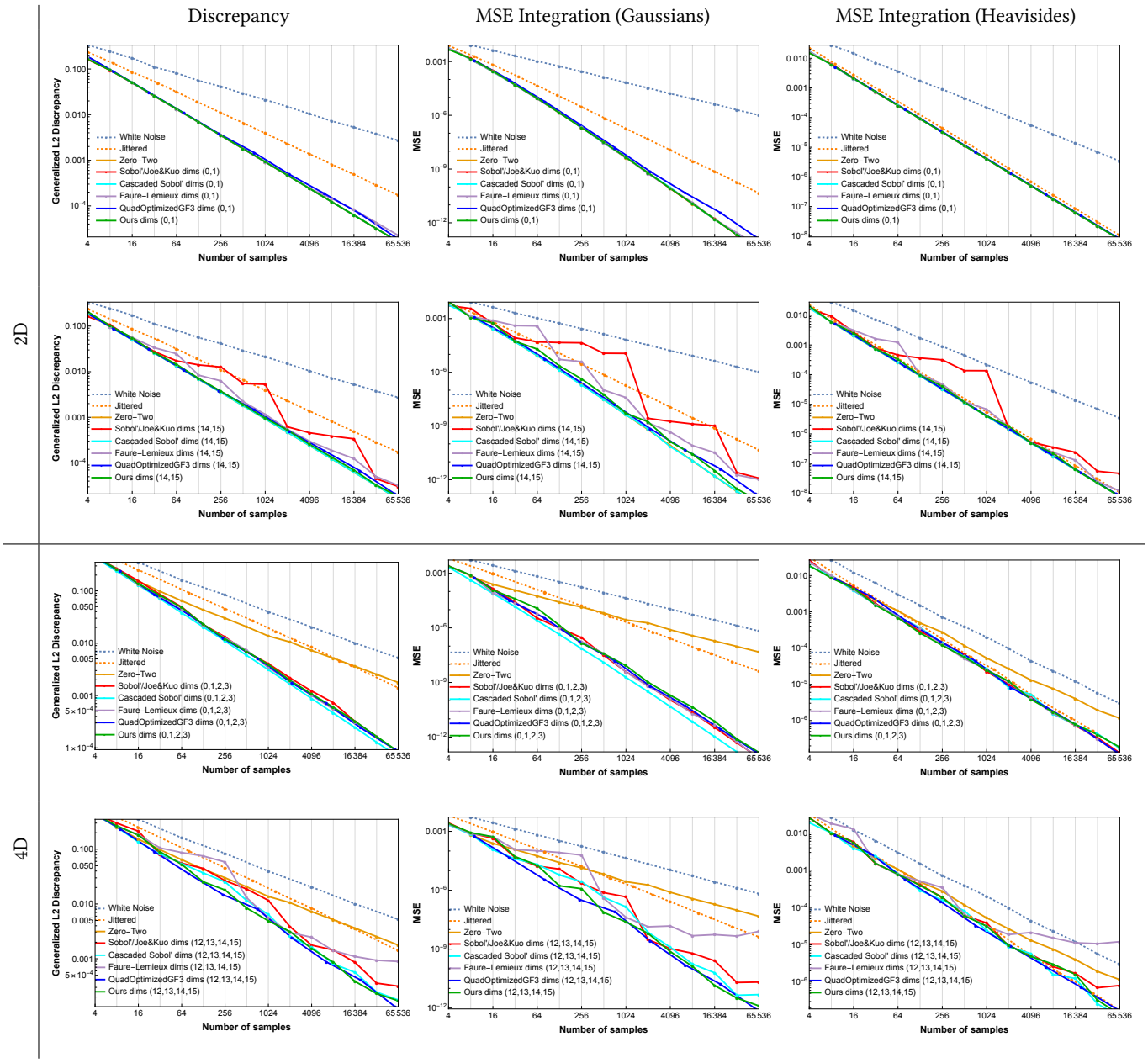


Fig. 9. In 2D and 4D, we evaluate the samplers quality with respect to the generalized L_2 discrepancy measure [Hickernell 1998] and integration errors (MSE) for random Gaussians and random Heavisides integrands (results averaged over 64 Owen-scrambled point sets). Although Sobol' [1967]/Joe and Kuo [2008] and Faure and Lemieux [2016] sequences are of high quality for the pair $(0,1)$ and the quadruple $(0,1,2,3)$, higher discrepancies and integration errors can be observed for the pair $(14,15)$ and the quadruple $(12,13,14,15)$. In contrast, quad-optimized LDS in $GF(3)$ [Ostromoukhov et al. 2024] and our sequences show comparable results, with our sequences more easily computed in $GF(2)$.

6 Conclusions

We designed a theoretical construction of 2D Sobol' sequences with $t = 1$ using p and $p^2 + p + 1$, while remaining low-discrepancy in higher dimensions. In practice, we found many solutions of unique characteristic matrices, in contrast to the unique solution for $t = 0$. We used 346 such pairs to produce a 692D sequence having at most $t = 1$ in 2D consecutive projections. In the process of proving $t = 1$, we discovered a new recursive construction for Sobol' matrices and for characteristic matrices. However, the availability of pairs of irreducible polynomials in the form p and $p^2 + p + 1$ is limited, and their degrees quickly increase. In practice, we use polynomials of

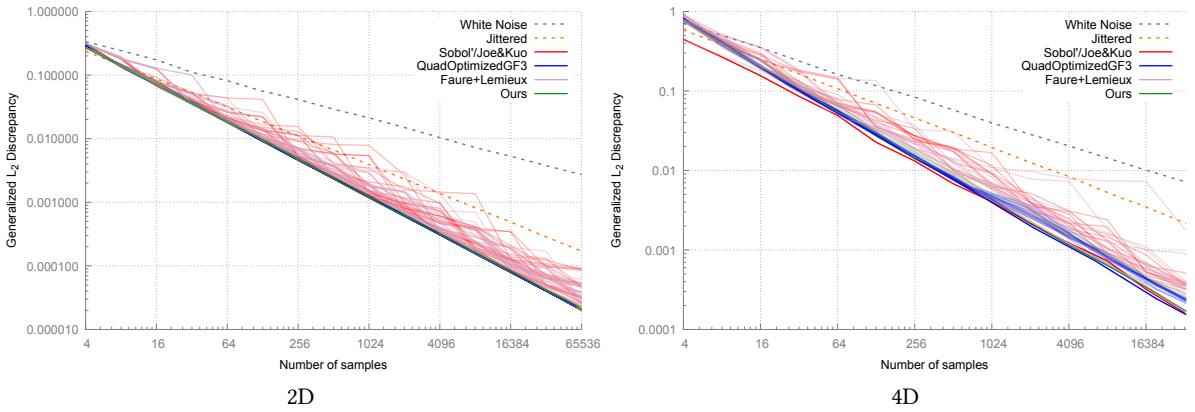


Fig. 10. Generalized L_2 discrepancy [Hickernell 1998] of consecutive 2D pairs (left) and quadruples of dimensions (right) of the first 36 dimensions of Sobol' using tables of Joe and Kuo [2008] (red), quad-optimized projection in $GF(3)$ [Ostromoukhov et al. 2024] (blue), Faure and Lemieux [2016] (magenta), and our sequences (green). We observe comparable results to the quad-optimized projection in $GF(3)$ while staying in $GF(2)$, both improving over Joe and Kuo.

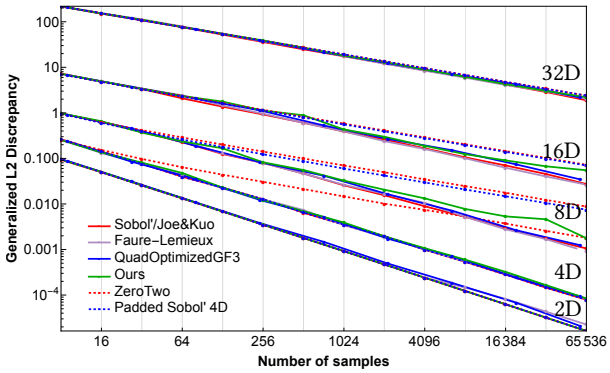


Fig. 11. For (t, s)-sequences only, we compare their generalized L_2 discrepancy in higher dimensions (from 2D to 32D, by increasing order of the polynomials). We observe similar results for all LDS sequences, while our sequence has highly uniform 2D projections (see Fig. 10-left). ZeroTwo [Pharr et al. 2023] and Padded 4D [Burley 2020] are not LDS in higher dimensions and thus do not offer the same convergence rate.

up to degree $2e = 32$ to produce 692 dimensions, while the construction of Faure and Lemieux [2016] uses at maximum polynomials of degree 13 to produce 1377 dimensions. While low-degree polynomials may appear desirable since they are guaranteed to reduce t for high-dimensional integration problems, as t is bounded by sums of polynomial degrees, this does not mean that t is necessarily large when the degree is large (in fact, our solution could lead to $t = 1$ in 2D for arbitrarily large polynomial degrees). We have found that the quality of our sequence remains competitive for moderately high-dimensional integration problems arising in path tracing, despite our use of higher-degree polynomials. Our use of a base-2 construction remains an advantage in rendering where efficiency is critical, and base-2 allows for both efficient sampling and Owen scrambling [Burley 2020; Owen 1995]. Our sampler produces a sequence, which is ideal for progressive rendering. Our use of standard Sobol' construction makes integration into existing renderers already supporting Sobol' extremely lightweight. We nevertheless intend to explore $b > 2$ within our framework to discover $t = 0$ sequences in higher dimensions, which remains a gold standard for numerical integration.

Acknowledgments

This work was partially funded by ANR-20-CE45-0025 (MoCaMed), by ANR-22-CE46-000 (StableProxies), and donations from Adobe Inc.

References

Abdalla GM Ahmed, Mikhail Skopenkov, Markus Hadwiger, and Peter Wonka. 2023. Analysis and synthesis of digital dyadic sequences. *ACM Transactions on Graphics (TOG)* 42, 6 (2023), 1–17.

Abdalla GM Ahmed and Peter Wonka. 2020. Screen-space blue-noise diffusion of Monte Carlo sampling error via hierarchical ordering of pixels. *ACM Transactions on Graphics (TOG)* 39, 6 (2020), 1–15.

Brent Burley. 2020. Practical hash-based Owen scrambling. *Journal of Computer Graphics Techniques (JCGT)* 10, 4 (2020), 29.

Per Christensen, Julian Fong, Jonathan Shade, Wayne Wooten, Brenden Schubert, Andrew Kensler, Stephen Friedman, Charlie Kilpatrick, Cliff Ramshaw, Marc Bannister, et al. 2018. Renderman: An advanced path-tracing architecture for movie rendering. *ACM Transactions on Graphics (TOG)* 37, 3 (2018), 1–21.

Josef Dick and Friedrich Pillichshammer. 2010. *Digital Nets and Sequences: Discrepancy Theory and Quasi–Monte Carlo Integration.* Cambridge University Press.

Henri Faure. 1982. Discrépance de suites associées à un système de numération (en dimension s). *Acta Arithmetica* 41, 4 (1982), 337–351.

Henri Faure and Christiane Lemieux. 2016. Irreducible Sobol'sequences in prime power bases. *Acta Arithmetica* 173, 1 (2016), 59–80.

Henri Faure and Christiane Lemieux. 2019. Implementation of irreducible Sobol'sequences in prime power bases. *Mathematics and Computers in Simulation* 161 (2019), 13–22.

Fred Hickernell. 1998. A generalized discrepancy and quadrature error bound. *Mathematics of computation* 67, 221 (1998), 299–322.

Roswitha Hofer and Kosuke Suzuki. 2019. A complete classification of digital (0, 3)-nets and digital (0, 2)-sequences in base 2. *Uniform distribution theory* 14, 1 (2019), 43–52.

Wojciech Jarosz, Afnan Enayet, Andrew Kensler, Charlie Kilpatrick, and Per Christensen. 2019. Orthogonal array sampling for Monte Carlo rendering. In *Computer Graphics Forum*, Vol. 38. Wiley Online Library, 135–147.

Stephen Joe and Frances Y Kuo. 2008. Constructing Sobol sequences with better two-dimensional projections. *SIAM Journal on Scientific Computing* 30, 5 (2008), 2635–2654.

Alexander Keller. 2004. Myths of computer graphics. In *Monte Carlo and Quasi-Monte Carlo Methods 2004*. Springer, 217–243.

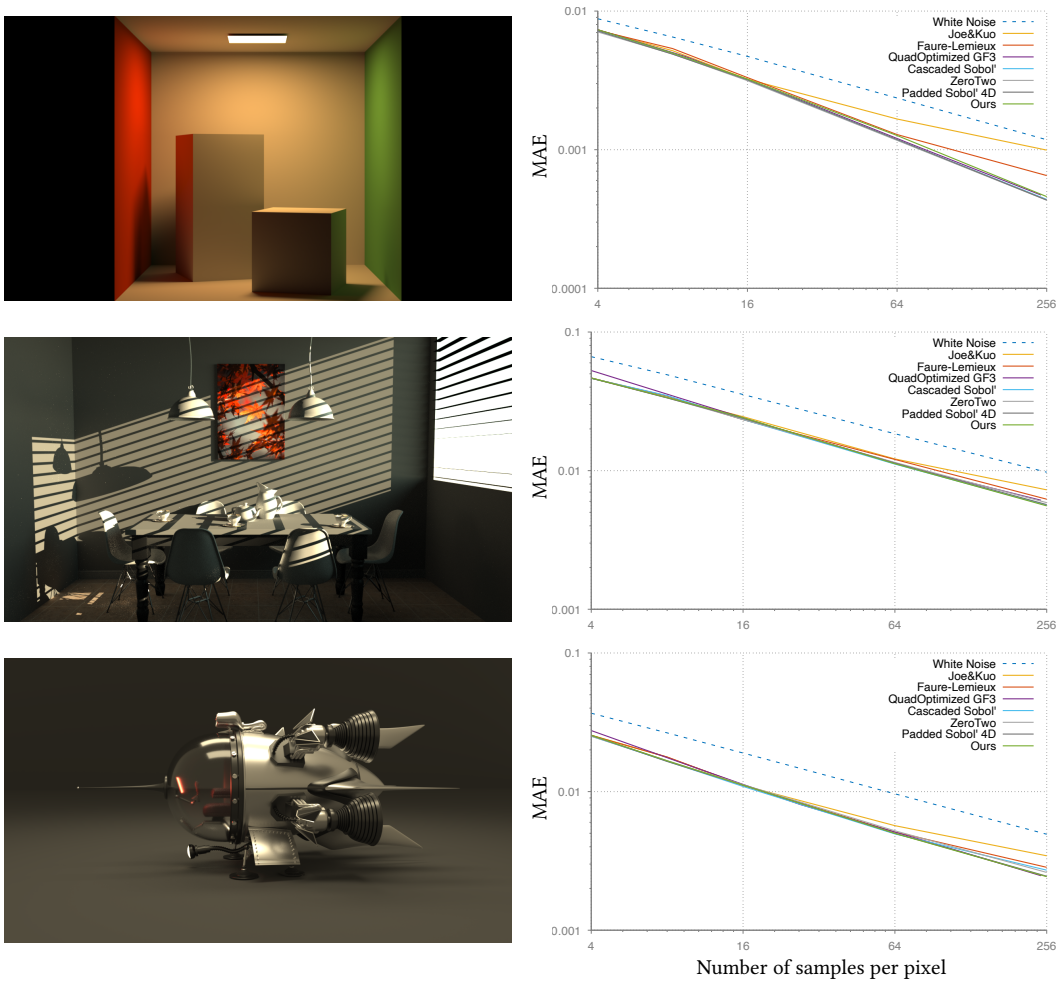


Fig. 12. Rendering results in 17D with 2 bounces (top and middle), and 35D with 5 bounces (bottom). We provide convergence graphs as a function of the number of samples per pixel (mean absolute error – MAE) showing that rendering can benefit from high-quality projections ($t = 1$ in our case) while being sequence for progressive rendering, contrary to Cascaded Sobol' [Paulin et al. 2021] (additional results in supplementary material). *Breakfast Room by blendswap user Wig42 and Spaceship by thecali, compiled by Benedikt Bitterli.*

Alexander Keller. 2013. Quasi-Monte Carlo image synthesis in a nutshell. In *Monte Carlo and Quasi-Monte Carlo Methods 2012*. Springer, 213–249.

Thomas Kollig and Alexander Keller. 2002. Efficient multidimensional sampling. In *Computer Graphics Forum*, Vol. 21. Wiley Online Library, 557–563.

Christiane Lemieux. 2009. *Monte Carlo and Quasi-Monte Carlo Sampling*. Vol. 20. Springer.

Carl D Meyer, Jr. 1973. Generalized inverses and ranks of block matrices. *SIAM J. Appl. Math.* 25, 4 (1973), 597–602.

Harald Niederreiter. 1988. Low-discrepancy and low-dispersion sequences. *Journal of number theory* 30, 1 (1988), 51–70.

Harald Niederreiter. 1992. *Random Number Generation and Quasi-Monte Carlo Methods*. SIAM.

Victor Ostromoukhov, Nicolas Bonneel, David Coeurjolly, and Jean-Claude Iehl. 2024. Quad-optimized low-discrepancy sequences. In *Proceedings of ACM SIGGRAPH*.

Art B Owen. 1995. Randomly permuted (t, m, s)-nets and (t, s)-sequences. In *Monte Carlo and Quasi-Monte Carlo Methods in Scientific Computing*. Springer, 299–317.

Loïs Paulin, Nicolas Bonneel, David Coeurjolly, Jean-Claude Iehl, Alex Keller, and Victor Ostromoukhov. 2022a. MatBuilder: Mastering Sampling Uniformity Over Projections. *ACM Transactions on Graphics (SIGGRAPH)* 41, 4 (Aug 2022).

Lois Paulin, Nicolas Bonneel, David Coeurjolly, Jean-Claude Iehl, Antoine Webanck, Mathieu Desbrun, and Victor Ostromoukhov. 2020. Sliced optimal transport sampling. *ACM Trans. Graph.* 39, 4 (2020), 99.

Loïs Paulin, David Coeurjolly, Nicolas Bonneel, Jean-Claude Iehl, Victor Ostromoukhov, and Alexander Keller. 2022b. Generator matrices by solving integer linear programs. In *International Conference on Monte Carlo and Quasi-Monte Carlo Methods in Scientific Computing*. Springer, 525–541.

Loïs Paulin, David Coeurjolly, Jean-Claude Iehl, Nicolas Bonneel, Alexander Keller, and Victor Ostromoukhov. 2021. Cascaded Sobol'Sampling. *ACM Transactions on Graphics (TOG)* 40, 6 (2021), 1–13.

Hélène Perrier, David Coeurjolly, Feng Xie, Matt Pharr, Pat Hanrahan, and Victor Ostromoukhov. 2018. Sequences with low-discrepancy blue-noise 2-D projections. In *Computer Graphics Forum*, Vol. 37. Wiley Online Library, 339–353.

Matt Pharr, Wenzel Jakob, and Greg Humphreys. 2023. *Physically based rendering: From theory to implementation* (4th ed.). MIT Press.

Bernhard Reinert, Tobias Ritschel, Hans-Peter Seidel, and Iliyan Georgiev. 2016. Projective blue-noise sampling. In *Computer Graphics Forum*, Vol. 35. Wiley Online Library, 285–295.

Neil James Alexander Sloane. 2001. The On-Line Encyclopedia of Integer Sequences. *https://oeis.org/A058943* (2001).

Il'ya Meerovich Sobol'. 1967. On the distribution of points in a cube and the approximate evaluation of integrals. *Zhurnal Vychislitel'noi Matematiki i Matematicheskoi Fiziki* 7, 4 (1967), 784–802.

A Additional derivations

A.1 Proofs of Eq. (10)

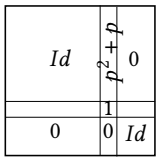
Starting from eq. 4 and $F_p^{-1} = (Id_e + R_{p,e}) \dots (Id_e + R_{p,2})$, we have:

$$F_{p^2+p+1}F_{p^2}^{-1} = \\ (Id_{2e} + R_{p^2+p+1,2}) \dots (Id_{2e} + R_{p^2+p+1,2e})(Id_{2e} + R_{p^2,2e}) \dots (Id_{2e} + R_{p^2,2})$$

To simplify the notations, we denotes $R'_k = (Id_{2e} + R_{p^2+p+1,k})$ and $R''_k = (Id_{2e} + R_{p^2,k})$. Hence, we have:

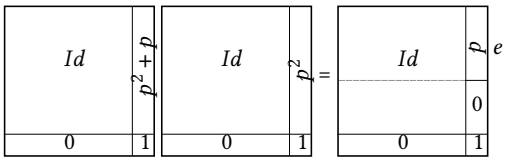
$$F_{p^2+p+1}F_{p^2}^{-1} = \\ \underbrace{R'_2 \dots R'_{e-1}}_{(i)} \underbrace{R'_e \dots R'_{2e-1} R'_{2e} R''_{2e} R''_{2e-1} \dots R''_e}_{(ii)} \underbrace{R''_{e-1} \dots R''_2}_{(iii)} \quad (14)$$

In the following, we will use this illustration for R'_k (the column of index k contains the $(k-1)$ highest degree coefficients of p^2+p+1):

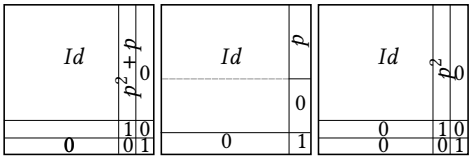


Note that by definition of R'_k and R''_k matrices, we can only consider polynomials p^2+p and p^2 respectively, as the constant factor is dropped by construction.

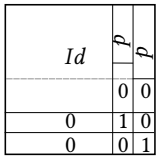
Let us first consider the first innermost product in part (ii) of Eq. (14) involving the p^2+p and p^2 polynomials $R'_{2e}R''_{2e}$:



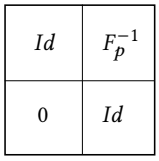
as p^2+p^2 coefficients cancel out for rows greater or equal to e. We denote by U_1 the resulting matrix. Let us now consider the product $U_2 = R'_{2e-1}\, U_1\, R''_{2e-1}$:



which simplifies to



If we repeat this process for all triplets of matrices $R'_k\, U_{2e-k}\, R''_k$ for the k indices of (ii), we end up with the matrix U_e:



Indeed, for each product $R'_k\, U_{2e-k}\, R''_k$, all p^2 coefficents vanish, leading to a triangular upper-right block with shifted p coefficients as in Eq. (7).

Let us now consider the product between (ii) and the (i) and (iii) parts in Eq. (14). First, we observe that

$$R''_{e-1}R''_{e-2} = \begin{array}{|c|c|} \hline Id & 0 \\ \hline 0 & Id \\ \hline \end{array}$$

By doing such products for all matrices of (iii), we obtain an upper-left block which corresponds to the first $e \times e$ entries of $F_{p^2+p}^{-1}$.

$$R''_{e-1} \dots R''_2 = \begin{pmatrix} F_{p^2}^{-1} & 0 \\ 0 & Id_e \end{pmatrix}.$$

For products in (i), we use the fact that

$$\left(R'_2 \dots R'_{e-1}\right)^{-1} = R'^{-1}_{e-1} \dots R'^{-1}_2 = R'_{e-1} \dots R'_2 = \begin{pmatrix} F_{p^2+p}^{-1} & 0 \\ 0 & Id_e \end{pmatrix},$$

as R'_k is its own inverse and using a similar construction as for (iii). Thus, using the inverse of a block matrix, we obtain

$$R'_2 \dots R'_{e-1} = \begin{pmatrix} F_{p^2+p} & 0 \\ 0 & Id_e \end{pmatrix},$$

which equals to $\begin{pmatrix} F_{p^2} & 0 \\ 0 & Id_e \end{pmatrix}$ as no coefficients for the p term are present in the upper-left block.

We finally have

$$\begin{aligned} F_{p^2+p+1}F_{p^2}^{-1} &= \begin{pmatrix} F_{p^2} & 0 \\ 0 & Id_e \end{pmatrix} \begin{pmatrix} Id_e & F_p^{-1} \\ 0 & Id_e \end{pmatrix} \begin{pmatrix} F_{p^2}^{-1} & 0 \\ 0 & Id_e \end{pmatrix} \\ &= \begin{pmatrix} F_{p^2} & 0 \\ 0 & Id_e \end{pmatrix} \begin{pmatrix} F_{p^2}^{-1} & F_p^{-1} \\ 0 & Id_e \end{pmatrix} \\ &= \begin{pmatrix} Id_e & F_p \\ 0 & Id_e \end{pmatrix}. \end{aligned}$$

which concludes Eq. (10). The last step uses the observation that, for the upper-right block, $F_{p^2}F_p^{-1} = \left(\left(F_{p^2}F_p^{-1}\right)^{-1}\right)^{-1} = \left(F_pF_{p^2}^{-1}\right)^{-1} = \left(F_pF_p^{-1}F_p^{-1}\right)^{-1} = F_p$.

A.2 Proofs of Eq. (11)

First, combining Eq. (9) and (10), we have:

$$F_{p^2+p+1}F_{p^2}^{-1}D_{p^2}^{-1} = \begin{pmatrix} Id_e & F_p \\ 0 & Id_e \end{pmatrix}\begin{pmatrix} Id_e & Q_p \\ 0 & F_p^{-1} \end{pmatrix}\begin{pmatrix} D_p^{-1} & 0 \\ 0 & D_p^{-1} \end{pmatrix} \quad (15)$$

$$= \begin{pmatrix} Id_e & Q_p + Id_e \\ 0 & F_p^{-1} \end{pmatrix}\begin{pmatrix} D_p^{-1} & 0 \\ 0 & D_p^{-1} \end{pmatrix} \quad (16)$$

$$= \begin{pmatrix} Id_e & Q_p \\ 0 & F_p^{-1} \end{pmatrix}\begin{pmatrix} D_p^{-1} & D_p^{-1} \\ 0 & D_p^{-1} \end{pmatrix} \quad (17)$$

$$= \begin{pmatrix} Id_e & Q_p \\ 0 & Id_e \end{pmatrix}\begin{pmatrix} D_p^{-1} & 0 \\ 0 & D_p^{-1} \end{pmatrix}\begin{pmatrix} Id_e & Id_e \\ 0 & Id_e \end{pmatrix} \quad (18)$$

$$= D_{p^2}^{-1}\begin{pmatrix} Id_e & Id_e \\ 0 & Id_e \end{pmatrix}, \quad (19)$$

leading to Eq. (11). Starting from Eq. (16), we also have

$$F_{p^2+p+1}F_{p^2}^{-1}D_{p^2}^{-1} = \begin{pmatrix} Id_e & Q_p + Id_e \\ 0 & F_p^{-1} \end{pmatrix}\begin{pmatrix} D_p^{-1} & 0 \\ 0 & D_p^{-1} \end{pmatrix} \quad (20)$$

$$= \begin{pmatrix} Id_e & Q_{p+1} \\ 0 & F_p^{-1} \end{pmatrix}\begin{pmatrix} D_p^{-1} & 0 \\ 0 & D_p^{-1} \end{pmatrix}, \quad (21)$$

that will be used later.

A.3 Proofs of Eq. (12)

Let us now prove the following statement:

$$(Q_{p^2} + Q_{p^2+p+1}F_{p^2+p+1}F_{p^2}^{-1})D_{p^2}^{-1} = D_{p^2}^{-1}\begin{pmatrix} Id_e & Id_e \\ Id_e & 0 \end{pmatrix}.$$

From now on, we make explicit the size of the matrices using $[e]$ or $[2e]$ superscripts. First, by definition, $Q_{p^2}^{[2e]}$ is

$$Q_{p^2}^{[2e]} = \begin{pmatrix} a_0 & 0 & 0 & \dots & 0 \\ 0 & a_0 & 0 & \dots & 0 \\ a_1 & 0 & a_0 & \dots & 0 \\ 0 & a_1 & 0 & \dots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ a_{e-1} & 0 & a_{e-2} & \dots & a_0 \end{pmatrix}. \quad (22)$$

We decompose $Q_{p^2}^{[2e]}$ into $e \times e$ blocks:

$$Q_{p^2}^{[2e]} = \begin{pmatrix} Q_{p^2}^{[e]} & 0 \\ \widetilde{Q}_{p^2}^{[e]} & Q_{p^2}^{[e]} \end{pmatrix}. \quad (23)$$

Similar to $Q_{p^2}^{[2e]}$, $\widetilde{Q}_{p^2}^{[e]}$ is also Toeplitz. Furthermore, we have

$$Q_{p+q}^{[e]} = Q_p^{[e]} + Q_q^{[e]} \quad \text{and} \quad Q_{pq}^{[e]} = Q_p^{[e]}Q_q^{[e]},$$

for any polynomial p and q of degree e. The same holds for $\widetilde{Q}_{p+q}^{[e]}$ and $\widetilde{Q}_{pq}^{[e]}$ matrices. Now,

$$(Q_{p^2} + Q_{p^2+p+1}F_{p^2+p+1}F_{p^2}^{-1})D_{p^2}^{-1} =$$
$$= Q_{p^2}D_{p^2}^{-1} + Q_{p^2+p+1}F_{p^2+p+1}F_{p^2}^{-1}D_{p^2}^{-1}$$

using Eq. (9) and 21 with $T = \begin{pmatrix} D_p^{-1} & 0 \\ 0 & D_p^{-1} \end{pmatrix}$

$$= \left(\begin{pmatrix} Q_{p^2}^{[e]} & 0 \\ \widetilde{Q}_{p^2}^{[e]} & Q_{p^2}^{[e]} \end{pmatrix}\begin{pmatrix} Id_e & Q_p^{[e]} \\ 0 & \widetilde{Q}_p^{[e]} \end{pmatrix} + \begin{pmatrix} Q_{p^2+p+1}^{[e]} & 0 \\ \widetilde{Q}_{p^2+p+1}^{[e]} & Q_{p^2+p+1}^{[e]} \end{pmatrix}\begin{pmatrix} Id_e & Q_{p+1}^{[e]} \\ 0 & \widetilde{Q}_{p+1}^{[e]} \end{pmatrix}\right)T. \quad (24)$$

First, we observe that $\widetilde{Q}_p^{[e]} = \widetilde{Q}_{p+1}^{[e]}$. The first factor can be rewritten

$$\begin{pmatrix} Q_{p^2}^{[e]} & Q_{p^3}^{[e]} \\ \widetilde{Q}_{p^2}^{[e]} & \widetilde{Q}_{p^2}^{[e]}Q_p^{[e]} + Q_{p^2}^{[e]}\widetilde{Q}_p^{[e]} \end{pmatrix} + \begin{pmatrix} Q_{p^2+p+1}^{[e]} & Q_{p^3+1}^{[e]} \\ \widetilde{Q}_{p^2+p+1}^{[e]} & \widetilde{Q}_{p^2+p+1}^{[e]}Q_{p+1}^{[e]} + Q_{p^2+p+1}^{[e]}\widetilde{Q}_{p+1}^{[e]} \end{pmatrix},$$

since $Q_{p^2}^{[e]}Q_p^{[e]} = Q_{p^3}^{[e]}$ and $Q_{p^2+p+1}^{[e]}Q_p^{[e]} = Q_{p^3+p^2+p}^{[e]}$. Furthermore, for any polynomial p and q of degree e, we have

$$Q_{pq}^{[2e]} = Q_p^{[2e]}Q_q^{[2e]} = \begin{pmatrix} Q_p^{[e]} & 0 \\ \widetilde{Q}_p^{[e]} & Q_p^{[e]} \end{pmatrix}\begin{pmatrix} Q_q^{[e]} & 0 \\ \widetilde{Q}_q^{[e]} & Q_q^{[e]} \end{pmatrix} = \begin{pmatrix} Q_{pq}^{[e]} & 0 \\ \widetilde{Q}_p^{[e]}Q_q^{[e]} + Q_p^{[e]}\widetilde{Q}_q^{[e]} & Q_{pq}^{[e]} \end{pmatrix}.$$

Hence, the first factor of Eq. (24) is

$$\begin{pmatrix} Q_{p^2}^{[e]} & Q_{p^3}^{[e]} \\ \widetilde{Q}_{p^2}^{[e]} & \widetilde{Q}_{p^3}^{[e]} \end{pmatrix} + \begin{pmatrix} Q_{p^2+p+1}^{[e]} & Q_{p^3+1}^{[e]} \\ \widetilde{Q}_{p^2+p+1}^{[e]} & \widetilde{Q}_{p^3+1}^{[e]} \end{pmatrix} = \begin{pmatrix} Q_{p+1}^{[e]} & Q_1^{[e]} \\ \widetilde{Q}_{p+1}^{[e]} & \widetilde{Q}_{p^3}^{[e]} + \widetilde{Q}_{p^3+1}^{[e]} \end{pmatrix} = \begin{pmatrix} Q_{p+1}^{[e]} & Id_e \\ F_p^{-1} & 0 \end{pmatrix},$$

using the fact that $\widetilde{Q}_p^{[e]} = F_p^{-1}$ from the construction of both matrices.

Finally,

$$
\begin{aligned}
(Q_{p^2} + Q_{p^2+p+1}F_{p^2+p+1}F_{p^2}^{-1})D_{p^2}^{-1} &= \begin{pmatrix} Q_{p+1}^{[e]} & Id_e \\ F_p^{-1} & 0 \end{pmatrix} T \\
&= \begin{pmatrix} Q_{p+1}^{[e]} & Id_e \\ F_p^{-1} & 0 \end{pmatrix} \begin{pmatrix} D_p^{-1} & 0 \\ 0 & D_p^{-1} \end{pmatrix} \\
&= \begin{pmatrix} Q_p^{[e]} + Id_e & Id_e \\ F_p^{-1} & 0 \end{pmatrix} \begin{pmatrix} D_p^{-1} & 0 \\ 0 & D_p^{-1} \end{pmatrix} \\
&= \begin{pmatrix} Id_e & Q_p^{[e]} + Id_e \\ 0 & F_p^{-1} \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} D_p^{-1} & 0 \\ 0 & D_p^{-1} \end{pmatrix} \\
&= D_{p^2}^{-1} \begin{pmatrix} Id_e & Id_e \\ Id_e & 0 \end{pmatrix},
\end{aligned}
$$

which concludes the proof of Eq. (12).

A.4 $(1,2)-$sequences and corank 1 submatrices of K

Let us consider two Sobol' matrices M_p and M_q of size $m \times m$ forming a $(t, m, 2)$-net. We denote $K = M_q M_p^{-1}$. First we remind that the pairs of matrices (M_p, M_q) and (Id_m, K) generate the same point set (up to indices permutation). Let $\mathcal{K}_k^t$ the $(m-t) \times m$ matrix consisting of the first k rows of Id_m and the first $m-k-t$ rows of K:

$$
\mathcal{K}_k^t = \begin{array}{c|c|c} & k & m-k \\ \hline k & Id_k & 0 \\ \hline m-k-t & K' & K'' \end{array}
$$

Lemma A.1 (Niederreiter [1992] (p. 73) and Paulin et al [2022b]). *M_p and M_q is a $(t, m, 2)-$net if and only if for all $k \in \{1, \dots, m\}$, $\mathcal{K}_k^t$ has corank t.*

From block-wise rank computation (the corank of a block triangular matrix with one full rank diagonal block is the corank of the other diagonal block [Meyer 1973]), we have

$$\text{corank}(\mathcal{K}_k^t) = \text{corank}(K'') .$$

Focusing on $(1,2)$-sequences, matrices K'' for all m and all k of size $(m-k-1) \times (m-k)$ are exactly the $T^{j,w}$ matrices involved in the property $\mathcal{P}$ (see Sect. 4.5). As a consequence, if each such matrices T has corank 1, we can conclude that K characterizes a $(1,2)-$sequence.