Sitzungsber. Abt. II (2005) 214: 133–140

Sitzungsberichte
Mathematisch-naturwissenschaftliche Klasse Abt. II
Mathematische, Physikalische und Technische Wissenschaften

A Small Taxonomy of Integration Node Sets

By

Gottlieb Pirsic

(Vorgelegt in der Sitzung der math.-nat. Klasse am 13. Oktober 2005
durch das k. M. Robert F. Tichy)

Abstract

Several digital point sets used in quasi-Monte Carlo integration can be regarded as special cases of or having common special cases with a recently introduced construction, namely cyclic digital nets. We will in particular investigate the relationships to polynomial lattice rules, Korobov-type polynomial lattice rules and constacyclic shift-nets.

1. Introduction

In high-dimensional numerical integration, an appropriate choice of node set becomes increasingly more important as the dimension of the problem gets larger. One way to assess the quality of a node set is by the measure of uniformity called *discrepancy*, which is a worst-case error of the numerical integration of characteristic functions of intervals.

A particular efficient way to obtain point sets with low discrepancy is to use so-called digital nets. Several well-investigated construction methods exist, e.g. polynomial lattice rules, which can be defined to model a polynomial analogue to Kronecker sequences (incidentally, rank 1 lattice rules, i.e. finite rational Kronecker sequences, can be regarded as digital $(0, 1, s)$-nets over a residue class ring). Other digital net constructions, such as shift-nets, have yielded very good results (with respect to their quality parameter) in computer searches.

This article aims to clear up the relations of the above-mentioned constructions and the more recent constructions of cyclic digital nets and their generalization, hyperplane nets.

2. Cyclic Digital Nets and Hyperplane Nets

The notion of cyclic digital nets was first introduced by Niederreiter in [2].

Definition 1 (Cyclic Digital Net, 1st Definition (Deprecated)). Let integers $m \geq 1, s \geq 2$ and a finite field $\mathbb{F}_q$ be given. Fix an element $\alpha \in \mathbb{F}_{q^m}$ and consider the set of polynomials

$$\mathcal{P}_\alpha := \{f \in \mathcal{P}, f(\alpha) = 0\} \quad \subseteq \quad \mathcal{P} := \{f \in \mathbb{F}_{q^m}[x], \deg(f) < s\}.$$

For each $j = 1, \ldots, s$ choose an ordered basis $\mathcal{B}_j$ of $\mathbb{F}_{q^m}$ over $\mathbb{F}_q$ and define ϕ as the mapping

$$\phi: f(x) = \sum_{j=1}^{s} \gamma_j x^{j-1} \in \mathcal{P}_\alpha \mapsto (\gamma_{1,1}, \ldots, \gamma_{1,m}, \ldots, \gamma_{s,1}, \ldots, \gamma_{s,m}) \in \mathbb{F}_q^{ms},$$

where $(\gamma_{j,1}, \ldots, \gamma_{j,m})$ is the coordinate vector of γ_j with respect to the chosen basis $\mathcal{B}_j$.

We denote by $\mathcal{C}_\alpha$ the orthogonal subspace in $\mathbb{F}_q^{ms}$ of the image $\mathcal{N}_\alpha := \phi(\mathcal{P}_\alpha)$. Let

$$C_\alpha = (C_1^\top \cdots C_s^\top) \in \mathbb{F}_q^{m \times sm}$$

be a matrix whose row space is $\mathcal{C}_\alpha$. Then the C_j are the generator matrices of a *cyclic digital net*.

It has been established in [4] that there is a both computationally more convenient and perhaps theoretically more transparent way to define and investigate cyclic digital nets. It uses a representation of $\mathbb{F}_{q^m}$ in the matrix ring $\mathbb{F}_q^{m \times m}$. We define this representation with the following lemma slightly more general, not only for fields but also arbitrary polynomial residue class rings. The notations introduced in the lemma (specifically the maps ψ, Ψ) will be used throughout the paper. Also we use the notation $\mathbb{F}_q[x]_\tau := \mathbb{F}_q[x]/\tau(x)\mathbb{F}_q[x]$ in analogy to the common integer residue class ring notation $\mathbb{Z}_m := \mathbb{Z}/m\mathbb{Z}$.

Lemma 1. *Let $\mathbb{F}_q$ be a finite field and $E = \mathbb{F}_q[x]_\tau, \tau(x) \in \mathbb{F}_q[x]$, an arbitrary polynomial residue class ring with $\tau(x)$ of degree $m > 1$. Let θ be the residue class of x in E, let*

$$\theta^m = t_0 + t_1\theta + \cdots + t_{m-1}\theta^{m-1}, \quad t_i \in \mathbb{F}_q$$

and define

$$\Theta := \begin{pmatrix} 0 & 0 & 0 & \cdots & t_0 \\ 1 & 0 & 0 & \cdots & t_1 \\ 0 & 1 & 0 & \cdots & t_2 \\ & \vdots & & \ddots & \vdots \\ 0 & \cdots & 0 & 1 & t_{m-1} \end{pmatrix}.$$

Furthermore, consider E as an m-dimensional $\mathbb{F}_q$-vector space with the ordered basis $\{1, \theta, \ldots, \theta^{m-1}\}$ by the map $\psi: E \to \mathbb{F}_q^m$,

$$\psi(g) := (g_0, \ldots, g_{m-1}), \qquad g = \sum_{i=0}^{m-1} g_i \theta^i \in E, \quad g_i \in \mathbb{F}_q.$$

Finally define a map $\Psi: E \to \mathbb{F}_q^{m \times m}$ by

$$\Psi(g) := \sum_{i=0}^{m-1} g_i \Theta^i,$$

g as above. Then, for any $a, g \in E$

$$\psi(ag) = \Psi(a)\psi(g).$$

Proof. This follows quite easily by first showing the lemma for a, g equal to powers of θ and then using linearity. □

The result shown in [4] regarding cyclic digital nets is as follows:

Theorem 1. *Let $m, s, \mathbb{F}_q$ and $\alpha \in \mathbb{F}_{q^m} = \mathbb{F}_q[x]_\tau$ with an irreducible $\tau \in \mathbb{F}_q[x]$ be given and define s matrices $B_j = (\psi(b_{j,1}), \ldots, \psi(b_{j,m}))^{-1}$, where the $b_{j,l}$ constitute the chosen basis $\mathcal{B}_j$. Then the generator matrices of the net are given by $C_j = (\Psi(\alpha)^{j-1} B_j)^\top$, $j = 1, \ldots, s$. Furthermore it follows that C_j is regular for $j = 1, \ldots, s$.*

Apparently any set of regular matrices can be factored to conform to this scheme, i.e. given C_j, choosing $B_j = \Psi(\alpha)^{-j+1} C_j^\top$ yields C_j as a digital cyclic net generator matrix. There are situations, when this is not a problem, e.g. when we first choose some bases $\mathcal{B}_j$ and then search through all α to optimize some quality parameter of the ensuing net (this was done in [4]). But in most cases, it is preferable to consider a restricted version of the original definition, where only a constant fixed basis $\mathcal{B}_j = \mathcal{B}$ is allowed. This was proposed by Niederreiter in [3] and we will adopt this view in the following

Definition 2 (Cyclic Digital Nets, 2nd Definition). As Definition 1, but with $\mathcal{B}_j = \mathcal{B}$ for all $j = 1, \ldots, s$.

Actually we will make two more generalization steps from here: The first is to allow arbitrary polynomial residue class rings $\mathbb{F}_q[x]_\tau$ to stand in the place of $\mathbb{F}_{q^m}$ in Definition 1, and the second is to allow arbitrary α_i instead of only the powers α^{i-1}. This second step is a slightly generalized version of the hyperplane nets, defined in Definition 2.10 in [4].

Definition 3 (Cyclic Digital Nets, 3rd Definition). As Definition 2, but using an arbitrary polynomial residue class ring $\mathbb{F}_q[x]_\tau$ instead of $\mathbb{F}_{q^m}$.

Or, putting it differently, using the notation and prerequisites of Theorem 1, the generator matrices are given by $C_i = (\Psi(\alpha^{i-1})B)^\top$, $i = 1, \ldots, s$, with $\alpha \in E = \mathbb{F}_q[x]_\tau$, $\tau \in \mathbb{F}_q[x]$ and some fixed regular matrix $B \in E^{m \times m}$.

Definition 4 (Hyperplane Nets, 1st Definition). As Definition 2, but using different elements α_i in the place of the powers of α.

Or, putting it differently, using the notation and prerequisites of Theorem 1, the generator matrices are given by $C_i = (\Psi(\alpha_i)B)^\top$, $i = 1, \ldots, s$ with $\alpha_i \in \mathbb{F}_{q^m}$, and some fixed regular matrix $B \in \mathbb{F}_q^{m \times m}$.

(This is Definition 2.10 in [4].)

Definition 5 (Hyperplane Nets, 2nd Definition). As Definition 3, but using different elements α_i in the place of the powers of α.

Or, putting it differently, using the notation and prerequisites of Theorem 1, the generator matrices are given by $C_i = (\Psi(\alpha_i)B)^\top$, $i = 1, \ldots, s$ with $\alpha_i \in E = \mathbb{F}_q[x]_\tau$, $\tau \in \mathbb{F}_q[x]$ and some fixed regular matrix $B \in E^{m \times m}$.

Remark 1. The ''officially valid'' definitions of cyclic digital and hyperplane nets are the 2nd and 1st, respectively. The first definition of cyclic digital nets is deprecated for the reasons given above.

Note that Definitions 2, 3 and 5 are special cases of increasing generality (and Definition 1 is the most general).

$$\begin{aligned} \text{Cyc. Dig. Net, Def. 2} \quad &\subseteq \quad \text{Cyc. Dig. Net, Def. 3} \\ &\subseteq \text{Hyperplane Net} \quad (\subseteq \text{Cyc. Dig. Net, Def. 1}). \end{aligned}$$

(Cf. also Figs. 1 and 2.)

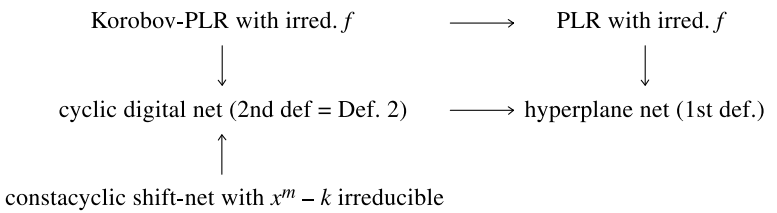

Fig. 1. The relations to the original definitions of cyclic digital and hyperplane nets

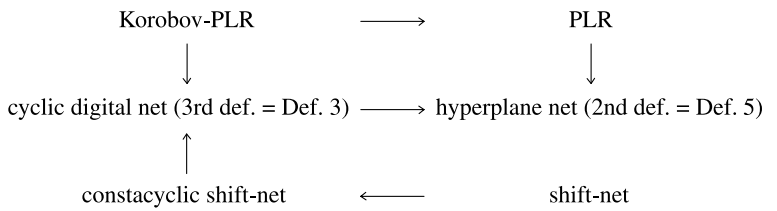

Fig. 2. The relations to the generalized definitions of cyclic digital and hyperplane nets

3. Polynomial Lattice Rules and Shift-Nets

Now we want to make the connection to the polynomial lattice rule (PLR) construction.

There are several equivalent definitions of PLR, first defined in [1]. We will use the approach by Hankel matrices.

Definition 6 (Polynomial Lattice Rules). Given polynomials $f, g_i \in \mathbb{F}_q[x]$, $\deg(f) = m - 1 \geq \deg(g_i), i = 1, \ldots, s$, if $g_i(x)/f(x) = \sum_{j > w_i} g_{i,j} x^{-j}, w_i \in \mathbb{Z}$ are the Laurent expansions in $1/x$, let generator matrices C_i be defined by the $m \times m$ Hankel matrices associated to the series of the coefficients. In detail,

$$C_i = \begin{pmatrix} g_{i,1} & g_{i,2} & \cdots & g_{i,m} \\ g_{i,2} & \iddots & g_{i,m} & \vdots \\ \vdots & g_{i,m} & \iddots & g_{i,2m-2} \\ g_{i,m} & \cdots & g_{i,2m-2} & g_{i,2m-1} \end{pmatrix}.$$

The corresponding digital net is called *a polynomial lattice rule*. The specific choice of $g_1 = 1, g_i = g_2^{i-1}, i = 3, \ldots, s$ is called a *Korobov-type polynomial lattice rule*.

We claim that

$$C_i = P\,\Psi(g_i(\theta)), \qquad P = \begin{pmatrix} 0 & \cdots & 0 & 1 \\ \vdots & \iddots & \iddots & f_1 \\ 0 & \iddots & \iddots & \vdots \\ 1 & f_1 & \cdots & f_{m-1} \end{pmatrix}$$

(i.e. P is the Hankel matrix associated to $1/f(x) = x^{-m} + \sum_{j>m} f_{j-m}x^{-j}$), where, following the notation and framework of the previous section, θ is the residue class of x in $\mathbb{F}_q[x]_f$.

Indeed, if $g_i(x) = \sum_{j=0}^{m-1} G_{i,j}x^j$, then the map associated to the first column of C_i is (by τ_m we denote the truncation map of the series to the vector of the first m positively indexed coefficients)

$$\frac{g_i(x)}{f(x)} = \sum_{j=0}^{m-1} G_{i,j}\frac{x^j}{f(x)} \mapsto \tau_m\left(\frac{g_i(x)}{f(x)}\right) := \begin{pmatrix} g_{i,1} \\ \vdots \\ g_{i,j} \\ \vdots \\ g_{i,m} \end{pmatrix} = P \begin{pmatrix} G_{i,0} \\ \vdots \\ G_{i,j} \\ \vdots \\ G_{i,m-1} \end{pmatrix}$$

since τ_m is linear and $P = (\tau_m(1/f(x)), \tau_m(x/f(x)), \ldots, \tau_m(x^{m-1}/f(x)))$. So altogether

$$\begin{aligned} C_i &= \left(\tau_m\left(\frac{g_i(x)}{f(x)}\right), \tau_m\left(\frac{xg_i(x)}{f(x)}\right), \ldots, \tau_m\left(\frac{x^{m-1}g_i(x)}{f(x)}\right)\right) \\ &= P(\phi(g_i(x) \bmod f(x)), \phi(xg_i(x) \bmod f(x)), \ldots, \\ &\quad \phi(x^{m-1}g_i(x) \bmod f(x))) \\ &= P\Psi(g_i), \end{aligned}$$

where ϕ maps polynomials to vectors of coefficients.

Now, since $C_i = C_i^\top$, we also have $C_i = \Psi(g_i)^\top P$, with a regular matrix P. The effect of P is only a reordering of the sequence associated to the generator matrices $\Psi(g_i)^\top$. Thus we arrive at

Theorem 2. *For $f \in \mathbb{F}[x], \deg(f) = m$ an arbitrary (i.e. not necessarily irreducible) polynomial, let $\theta = \bar{x}$ be the residue class of x in $\mathbb{F}_q[x]_f$, and C_i the generator matrices of a PLR associated to the polynomials $g_1, \ldots, g_s$, then C_iP^{-1} are identical to the generator matrices of the hyperplane net associated to the vector $(g_1(\theta), \ldots, g_s(\theta)) \in \mathbb{F}_{q^m}^s$ (and with the powers of θ as the choice for the ordered basis $\mathcal{B}$).*

As a special case, cyclic digital nets (understood under Definition 3) and Korobov-type PLR are equivalent in the same way. If f is chosen irreducible, this holds also for cyclic digital nets under Definition 2.

Schmid [5] introduced the so-called shift-net construction, which has yielded good results in computer searches. We can also incorporate this construction into the scheme of cyclic digital nets. In fact, we can even do this for a generalization of shift-nets (also investigated by Schmid, but as of yet unpublished), *constacyclic* shift-nets (the name is a reference to constacyclic codes in coding theory). Their construction is as follows: Starting from an appropriate matrix $C_1 = (\boldsymbol{c}_1, \ldots, \boldsymbol{c}_m)$ and some nonzero $k \in \mathbb{F}_q$, construct the matrices $C_2, \ldots, C_s, s \leq m$ by shifting the column vectors and multiplying the reentrant vectors by k, i.e.

$$C_i = (\boldsymbol{c}_i, \boldsymbol{c}_{i+1}, \ldots, \boldsymbol{c}_m, k\boldsymbol{c}1, \ldots, k\boldsymbol{c}_{i-1}).$$

(Clearly, plain shift-nets correspond to the case $k = 1$.)

If

$$\Theta := \left(\begin{array}{c|c} \mathbf{0} & k \\ \hline I_{m-1} & \mathbf{0} \end{array}\right)$$

(I_{m-1} the identity matrix of size $m-1$), then it is easy to see that $C_i = C_1\Theta^{i-1}$. Observe that Θ is the companion matrix to the polynomial $x^m - k$, i.e. in our notation $\Theta = \Psi(\theta)$ in the residue class ring $\mathbb{F}_q[x]/(x^m - k)\mathbb{F}_q[x]$. Our aim is to connect C_i with the transpose of $\Psi(\theta)$, as this is the form of the generator matrices of cyclic digital nets. In the following we will assume C_1 to be regular.

Let J be the skew diagonal identity matrix. For any matrix A, the transformation JAJ generates the ''point inverse'' (or ''doubly reflected'') matrix of A with respect to its entries. For Toeplitz matrices such as Θ this is identical to the transposed matrix, so

$$C_i = C_1\Theta^{i-1} = C_1(J\Theta^{(i-1)\top}J) = (JC_1^\top)^\top\Theta^{(i-1)\top}J = \Psi'(\theta^{i-1})^\top J,$$

where Ψ' is taken with respect to the basis of $\mathbb{F}_q(\theta)$ given by the columns of $(JC_1^\top)$, i.e. using the bijection ψ of the canonical basis of powers of θ, the ordered basis that is used in the construction is $\mathcal{B} = \{b_1, \ldots, b_m\}$, where $(JC_1^\top)^{-1} = (\psi(b_1), \ldots, \psi(b_m))$. We arrive at

Theorem 3. *If the first generator matrix of a constacyclic shift-net C_1 (with constant k) is regular, the resulting point set is a reordering of*

the cyclic digital net (*under Definition 3*) *associated to* θ *in the extension* $\mathbb{F}_q[x]/(x^m - k)\mathbb{F}_q[x]$ *and with the ordered basis* $\mathcal{B}$ *chosen as above*.

If $x^m - k$ *is irreducible*, *then this holds also for cyclic digital nets under Definition 2*.

We conclude by representing the found results in two graphs, with arrows representing the relation ''is a special case of''. In addition, the constructions in Fig. 1 are special cases of the constructions in the same place in Fig. 2.

References

[1] NIEDERREITER, H. (1992) Low-discrepancy point sets obtained by digital constructions over finite fields. Czech. Math. J. **42**: 143–166

[2] NIEDERREITER, H. (2004) Digital nets and coding theory. In: FENG, K. Q., NIEDEREITER, H., XING, C. P., (eds.) Coding, Cryptography and Combinatorics, pp. 247–257. Birkhäuser, Basel

[3] NIEDERREITER, H. (2005) Constructions of (t, m, s)-nets and (t, s)-sequences. Finite Fields Appl. **11**(3): 578–600

[4] DICK, J., PILLICHSHAMMER, F., PIRSIC, G. (2005) Cyclic Digital Nets, Hyperplane Nets and Multivariate Integration in Sobolev Spaces (submitted)

[5] SCHMID, W. CH. (1998) Shift-nets: A new class of binary digital (t, m, s)-nets. In: Monte Carlo and Quasi-Monte Carlo Methods 1996, Salzburg, pp. 369–381 (Lecture Notes in Statist., Vol. 127). Springer, New York

Author's address: Gottlieb Pirsic, J. Radon Institute (RICAM), Austrian Academy of Sciences, Altenberger Straße 69, 4020 Linz, Austria. E-Mail: Gottlieb.Pirsic@oeaw.ac.at.