Contents lists available at ScienceDirect

Discrete Applied Mathematics

journal homepage: www.elsevier.com/locate/dam

On finite pseudorandom binary lattices[☆]

Katalin Gyarmati[a,*], Christian Mauduit[b], András Sárközy[a]

[a] Eötvös Loránd University, Department of Algebra and Number Theory, H-1117 Budapest, Pázmány Péter sétány 1/C, Hungary

[b] Université Aix-Marseille, Institut de Mathématiques de Luminy, CNRS, UMR 7373, 165 avenue de Luminy, F-13288
Marseille Cedex 9, France

ARTICLE INFO

Article history:
Received 16 February 2015
Received in revised form 25 June 2015
Accepted 10 July 2015
Available online xxxx

Dedicated to the memory of Levon H. Khachatrian

Keywords:
Binary lattice
Pseudorandomness
Linear complexity
Families of lattices

ABSTRACT

Pseudorandom binary sequences play a crucial role in cryptography. The classical approach to pseudorandomness of binary sequences is based on computational complexity. This approach has certain weak points thus in the last two decades a new, more constructive and quantitative approach has been developed. Since multidimensional analogs of binary sequences (called binary lattices) also have important applications thus it is a natural idea to extend this new approach to the multidimensional case. This extension started with a paper published in 2006, and since that about 25 papers have been written on this subject. Here our goal is to present a survey of all these papers.

© 2015 Published by Elsevier B.V.

1. Introduction

Finite binary sequences possessing strong *pseudorandom* properties (briefly pseudorandom or just PR sequences) play a crucial role in cryptography, e.g. sequences of this type can be applied as *key* in the classical encrypting system called *Vernam cipher*. Moreover, the theory of pseudorandomness can be also utilized in *number theory*. Thus about 20 years ago Mauduit and Sárközy [35] (partly with coauthors) started to study pseudorandomness of binary *sequences*, and we developed a *quantitative* and *constructive* theory of this subject. (Recently Gyarmati [10] has published a comprehensive survey of the papers written on pseudorandomness of finite pseudorandom binary sequences.)

Multidimensional analogs of PR binary sequences (which we will call PR binary *lattices*) also have many applications in cryptography (e.g. in encrypting images and bit maps), steganography and watermarking. Few years ago we extended our theory of pseudorandomness from one dimension to the multidimensional case. The first paper [28] written on this subject appeared in 2006, and since that about 25 related papers have been published. Here our goal is to give a short *survey* of these papers (focusing mostly on our contribution).

2. Notation, definitions, measures of pseudorandomness, a construction

Let I_N^n denote the set of n-dimensional vectors all whose coordinates are in $\{0, 1, \dots, N-1\}$:

$$I_N^n = \left\{\underline{x} = (x_1, x_2, \dots, x_n) : x_1, \dots, x_n \in \{0, 1, \dots, N-1\}\right\}.$$

The set I_N^n is called the *n-dimensional N-lattice* or briefly (if n is fixed, usually as $n = 2$ or 3) *N-lattice*.

[☆] Research partially supported by Hungarian National Foundation for Scientific Research, Grants No. K100291 and NK104183, the János Bolyai Research Fellowship, the Agence Nationale de la Recherche grant ANR-10-BLAN 0103 called MUNUM and Ciencia sem Fronteiras, project PVE 407308/2013-0.

[*] Corresponding author.

E-mail addresses: gykati@cs.elte.hu (K. Gyarmati), mauduit@iml.univ-mrs.fr (C. Mauduit), sarkozy@cs.elte.hu (A. Sárközy).

http://dx.doi.org/10.1016/j.dam.2015.07.012
0166-218X/© 2015 Published by Elsevier B.V.

We remark that the points of I_N^n form an n-dimensional cube, in particular, for $n = 2$ a square:

$$\left\{\underline{x} = (x_1, x_2) : x_1, x_2 \in \{0, 1, \dots, N-1\}\right\}. \tag{2.1}$$

All our definitions and results to be presented later could be extended from squares to rectangles, i.e., from the N-lattice in (2.1) to the "(M, N)-*lattice*"

$$I_{(M,N)} = \left\{\underline{x} = (x_1, x_2) : x_1 \in \{0, 1, \dots, M-1\}, x_2 \in \{0, 1, \dots, N-1\}\right\}.$$

However, in all but one case we will stick to square (in general n-dimensional cube) N-lattices instead of using (M, N)-lattices since this makes the formulas slightly simpler. The only exception will be Section 7 on the linear complexity where it will be more advantageous to consider (M, N)-lattices.

Definition 1. A function of the type

$$\eta(\underline{x}) = \eta\big((x_1, \dots, x_n)\big) : I_N^n \to \{-1, +1\}$$

is called an *n-dimensional binary N-lattice* or briefly a *binary lattice*.

In other words, from an N-lattice I_N^n we get a binary lattice η if we assign -1 or $+1$ to each point (vector) of it.

Note that in the applications the binary sequences and binary lattices usually appear as *bit* sequences

$$S_N = (S_0, S_1, \dots, S_N) \in \{0, 1\}^N$$

and *bit* lattices

$$\delta : I_{M,N} \to \{0, 1\},$$

respectively. However, there is a natural trivial bijection between $\{-1, +1\}$ and $\{0, 1\}$, thus it makes no difference whether we use $-1, +1$ or bits when studying pseudorandomness of binary sequences and lattices. If we work with -1 and $+1$, then the expected value of the sum studied is usually 0 (due to cancellation) so that we need not carry a sometimes quite complicated main term. Thus we usually work with -1 and $+1$ instead of bits, and here in case of lattices we will also do this. Again, there will be just one exception: Section 7 where we will consider bit lattices instead of $\{-1, +1\}$ binary lattices.

Observe that in the $n = 1$ special case the binary N-lattices defined in Definition 1 are the binary *sequences* of length N. We will also need the following extension of Definition 1:

Definition 2. Let $\underline{u}_1, \underline{u}_2, \dots, \underline{u}_n$ be n linearly independent n-dimensional vectors over the field of the real numbers such that the ith coordinate of $\underline{u}_i$ is in $\{1, 2, \dots, N-1\}$ and the other coordinates of $\underline{u}_i$ are 0, so that $\underline{u}_i$ is of the form $(0, \dots, 0, z_i, 0, \dots, 0)$ with $z_i \in \{1, 2, \dots, N-1\}$. Let $t_1, t_2, \dots, t_n$ be integers with $0 \leqslant t_1, t_2, \dots, t_n < N$. Then the set

$$B_N^n = \left\{\underline{x} = x_1\underline{u}_1 + \dots + x_n\underline{u}_n : 0 \leqslant x_i|\underline{u}_i| \leqslant t_i (< N) \text{ for } i = 1, 2, \dots, n\right\}$$

is called an *n-dimensional box N-lattice* or briefly a *box N-lattice*.

In 2006 Hubert, Mauduit and Sárközy [28] introduced the following measures of pseudorandomness of binary lattices:

Definition 3. The *pseudorandom measure of order k* of the binary lattice $\eta : I_N^n \to \{-1, +1\}$ is defined by

$$Q_k(\eta) = \max_{B, \underline{d}_1, \dots, \underline{d}_k} \left| \sum_{x \in B} \eta(\underline{x} + \underline{d}_1)\eta(\underline{x} + \underline{d}_2) \dots \eta(\underline{x} + \underline{d}_k) \right|$$

where the maximum is taken over all distinct vectors $\underline{d}_1, \dots, \underline{d}_k$ with coordinates in $\{0, 1, \dots, N-1\}$ and all box N-lattices B such that $B + \underline{d}_1, \dots, B + \underline{d}_k \in I_N^n$.

Note that in the $n = 1$ special case this is the so-called *combined measure of order k* of the given binary *sequence* $\eta : I_N^1 \to \{-1, +1\}$ (see [35]).

It was shown in [28] that for a (truly) random lattice $\eta : I_N^n \to \{-1, +1\}$ the measure $Q_k(\eta)$ is around $N^{n/2}$:

Theorem 1. *If $k \in \mathbb{N}$ and $\varepsilon > 0$, then there are numbers $N_0 = N_0(k, \varepsilon)$ and $\delta = \delta(k, \varepsilon) > 0$ such that for $N > N_0$ we have*

$$P\big(Q_k(\eta) > \delta N^{n/2}\big) > 1 - \varepsilon$$

and

$$P\Big(Q_k(\eta) > \big(81kN^n \log N^n\big)^{1/2}\Big) < \varepsilon.$$

This was proved by the moment method as the analogous result in one dimension [5] (see also [4]), however, it makes a slight difficulty here that there is no natural ordering in I_N^n for $n > 1$. Thus η can be considered as a "good" PR lattice if $Q_k(\eta)$ is not much greater than $N^{n/2}$ (at least for "small" k values).

Please cite this article in press as: K. Gyarmati, et al., On finite pseudorandom binary lattices, Discrete Applied Mathematics (2015), http://dx.doi.org/10.1016/j.dam.2015.07.012

Download English Version:

https://daneshyari.com/en/article/4949841

Download Persian Version:

https://daneshyari.com/article/4949841

Daneshyari.com