PSEUDORANDOM BINARY FUNCTIONS ON ROOTED PLANE TREES

Katalin Gyarmati[*]
Affiliations: Eötvös Loránd University
Department of Algebra and Number Theory
H-1117 Budapest, Pázmány Péter sétány 1/C, Hungary
Pascal Hubert[†]
Laboratorie d'Analyse, Topologie et Probabilités
Faculté des Sciences de Saint Jérôme
Avenue Escadrille Normandie-Niemen
F-13397 Marseille Cedex 20, France
András Sárközy[‡]
Affiliations: Eötvös Loránd University
Department of Algebra and Number Theory
H-1117 Budapest, Pázmány Péter sétány 1/C, Hungary

Keywords and phrases: pseudorandom, binary function, rooted planar tree, correlation, Legendre symbol.

2010 Mathematics Subject Classification: Primary: 05C05, Secondary: 11K45.

[*]E-mail address: gykati@cs.elte.hu
[†]E-mail address: hubert@cmi.univ-mrs.fr
[‡]E-mail address: sarkozy@cs.elte.hu

Abstract

In an earlier paper the authors considered r-almost s-uniform trees, i.e. rooted planar trees T such that the root has r successors, and every other vertex has s successors. They considered binary functions $f : \mathcal{V}(T) \to \{-1, +1\}$ defined on the set $\mathcal{V}(T)$ of the vertices of such a tree T and studied the pseudorandomness of binary functions of this type. Here the authors extend the problem to general rooted plane trees: the measures of pseudorandomness of binary functions defined on trees of this type are introduced; the connection between these measures is analyzed; the size of these measures for truly random binary functions is studied; binary functions with strong pseudorandom properties are constructed; pseudorandom properties of important special binary functions are studied.

1. Introduction

Recently a new constructive approach has been developed to study pseudorandomness of binary sequences

$$E_N = \{e_1, \dots, e_N\} \in \{-1, +1\}^N.$$

In particular, first in [6] the following measures of pseudorandomness were introduced: the *well-distribution measure* of E_N is defined by

$$W(E_N) = \max_{a,b,t} \left| \sum_{j=0}^{t-1} e_{a+jb} \right|$$

where the maximum is taken over all $a, b, t \in \mathbb{N}$ with $1 \le a \le a + (t-1)b \le N$, the *correlation measure of order* k of E_N is defined as

$$C_k(E_N) = \max_{M,\mathbf{D}} \left| \sum_{n=1}^{M} e_{n+d_1} \dots e_{n+d_k} \right|$$

where the maximum is taken over all $\mathbf{D} = (d_1, \dots, d_k)$ and M such that $0 \le d_1 < \dots < d_k \le N - M$, and the *normality measure of order* k of E_N is defined as

$$N_k(E_N) =$$

$$\max_{\mathbf{X} \in \{-1,+1\}^k} \max_{0 < M < N+1-k} \left| |\{n : \ 0 \le n < M, \ (e_{n+1}, \dots, e_{n+k}) = \mathbf{X}\}| - \frac{M}{2^k} \right|.$$

Research partially supported by Hungarian National Foundation for Scientific Research, Grants No. K67676 and K72731, French-Hungarian exchange program F-33/2009, the Agence Nationale de la Recherche, grant ANR-10-BLAN 0103 MUNUM and the János Bolyai Research Fellowship.

Then the sequence E_N is considered to be a "good" pseudorandom sequence if both $W(E_N)$ and $C_k(E_N)$ (at least for "small" k) are "small" in terms of N; in particular, both are $o(N)$ as $N \to \infty$ (it was shown in [6] that the normality measures can be estimated in terms of the correlation measures). Indeed, later Cassaigne, Mauduit and Sárközy [2] proved that this terminology is justified since for almost all $E_N \in \{-1, +1\}^N$ both $W(E_N)$ and $C_k(E_N)$ are less than $N^{1/2}(\log N)^c$ (see also [1], [5]). It was also shown in [6] that the Legendre symbol forms a "good" pseudorandom sequence.

[6] was followed by numerous papers written on pseudorandomness of binary sequences. Later this theory of pseudorandomness has been extended from binary sequences to binary vectors, binary lattices, subsets of $\mathbb{Z}_n$, sequences of k symbols, etc. (see [4] for further references); in particular, in [4] we studied pseudorandomness of binary functions defined on *r-almost s-uniform trees* (some of the definitions and results presented in [4] will be recalled in Section 2 or later.) In this paper our goal is to continue the work initiated in [4] by extending the study of pseudorandomness of binary functions defined on trees from r-almost s-uniform trees to possibly general *rooted plane* (or ordered) *trees*.

2. Notation, terminology, definitions

Throughout this paper we will use the following notations:

Tree will always mean a finite rooted plane (or ordered) tree. We will use the words vertex (=node), root, successor (=child), leaf, path distance, height, subtree in the usual sense (see, e.g., [3], [8]). The vertices at distance k from the root are said to form the k-th *level* or $k+1$-st *row* of the tree (so that the 0-th level and 1st row consists of the single root). The number of successors of the vertex P will be called the degree of P and it will be denoted by $d(P)$ (this is called the out-degree of P and is denoted by $d^+(P)$ in [3]).

We will also introduce a few further definitions.

Definition 1. *If $r, s \in \mathbb{N}$ and $r \geq 2$, $s \geq 2$, then a tree is called an r-almost, s-uniform tree if the degree of the root is r, and the degree of every vertex different from the root and not in the last row is s. If $r = s$ then the tree is called s-uniform tree, and in the $r = s = 2$ special case the tree is called uniform binary tree.*

(It is explained in [4] why are we also considering the case when the degree of the root is different from the degree of the other vertices.)

Definition 2. *A subtree T' of the tree T is called a* proper subtree *if it can be obtained from T in the following way: the root of T' can be any vertex P of T. First we take all the successors of P, then we take all the successors of these successors, etc.; we stop after taking all the iterated successors at a certain (not necessarily the last) level.* (E.g., the black vertices in Figure 1 form a proper subtree.)

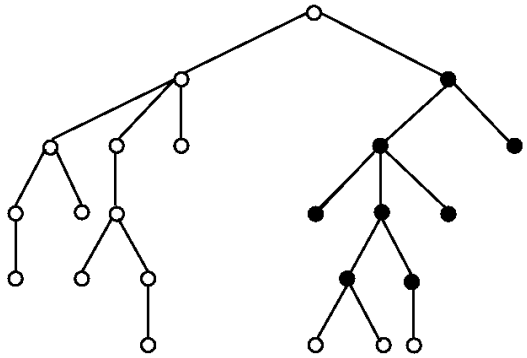

Figure 1.
A proper subtree

Note that in [4] we defined the notion of proper subtree in a slightly different way:

Definition 2'. *If T is an r-almost s-uniform tree, then a rooted subtree T' of T is called a* proper subtree *of T if either its root is the root of T and it is an r'-almost s-uniform tree for some $r' \le r$, or its root is different from the root of T and it is an s-uniform tree.*

Indeed, the successors of the root are handled in Definitions 2 and 2' in different ways: the $r' = r$ special case in Definition 2' would correspond to Definition 2. However, in the general case it seems more natural to handle the root in the same way as the other vertices, thus here we will use Definition 2 instead of Definition 2'.

Definition 3. *If T is a (rooted plane) tree and the set of its vertices is denoted by $\mathcal{V}(T)$ then a function f of the type $f : \mathcal{V}(T) \to \{-1, +1\}$ is called a* binary function *on T.*

If we want to introduce measures of pseudorandomness for general trees, then clearly we need some restrictions on the structure of the tree. Indeed, consider a tree which consists of a long path and some leafs branching off:

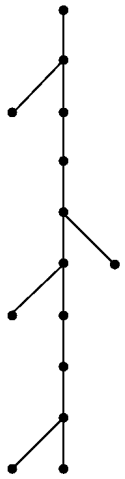

Figure 2.
An "irregular" tree

It might be very difficult to introduce any good measures of pseudorandomness for binary functions defined on trees of this type (in particular, it seems hopeless to define measures which take the vertices along the long "vertical" path into account in the same way as the many vertices with degree 0). Thus we will restrict ourselves to trees described in the following definition:

Definition 4. *If every vertex not in the last row has non-zero degree (i.e., all the leafs are in the last row) then the tree is called* regular.

We will also use the following notations:

The set of the vertices of a tree T will be denoted by $\mathcal{V} = \mathcal{V}(T)$. The number of these vertices will be denoted by $N = N(T) : \ N = N(T) = |\mathcal{V}|$. The height of the tree will be denoted by $h = h(T)$. We will denote the number of vertices in the i-th row (i.e., at the level $i-1$) by $y_i = y_i(T)$, and we will denote these vertices (moving from left to right which is possible since we consider rooted plane trees) by $P_T(i,1),\ P_T(i,2),\dots,P_T(i,y_i)$; if T is fixed then we will drop the subscript T. Clearly we have

$$N = N(T) = y_1 + y_2 + \cdots + y_{h+1}.$$

We will also use the following alternative notation for the vertices. The root is denoted by $Q_1 : \ Q_1 = P(1,1)$, the vertices in the second row by $Q_2, Q_3, \dots, Q_{y_2+1} : Q_2 = P(2,1)$, $Q_3 = P(2,2), \dots, Q_{y_2+1} = P(2,y_2)$, the vertices in the third row by

$Q_{y_2+2}, Q_{y_2+3}, \dots, Q_{y_2+y_3+1} : Q_{y_2+2} = P(3,1)$, $Q_{y_2+3} = P(3,2), \dots, Q_{y_2+y_3+1} = P(3,y_3)$ and so on; finally Q_N denotes the last vertex in the last row: $Q_N = P(h+1, y_{h+1})$.

To the binary function $f : \mathcal{V}(T) \to \{-1,+1\}$ defined on the (rooted plane) tree we will assign the unique binary sequence

$$E_N = E_N(f,T) = (e_1, e_2, \dots, e_N) \in \{-1,+1\}^N$$

defined by

$$e_n = f(Q_n) \quad \text{for } n = 1, 2, \dots, N.$$

Consider a path with endpoints Q_i, Q_j with $i < j$ (so that Q_i is the endpoint closer to the root). This path will be denoted by $\mathcal{P}(Q_i, Q_j)$.

Throughout the paper $\left(\frac{i}{p}\right)$ will denote the Legendre symbol.

3. The measures of pseudorandomness of binary functions on almost uniform trees.

Since our goal is to extend the definitions given in the special case of r-almost s-uniform trees in [4], thus first we will recall these definitions.

Definition 5. *The* well-distribution measure *of the binary function f over T is defined by*

$$\overline{W}(f,T) = W(E_N(f,T)).$$

Definition 6. *For $k \geq 2$ and $\ell \geq 2$ the* correlation measure $C_{k,\ell}(f,T)$ of height k and order ℓ *of f over T is defined in the following way: consider ℓ different isomorphic proper subtrees $T_1, T_2, \dots, T_\ell$ of height k of T, denote the set of their vertices by $\mathcal{V}_1, \mathcal{V}_2, \dots, \mathcal{V}_\ell$, and for $t = 1, 2, \dots, \ell$ let $\mathcal{V}_t = \{P_t(i,j) : \ i = 1, 2, \dots, k+1, \ j = 1, 2, \dots, q(i)\} = \{Q_{t,n} : n = 1, 2, \dots, N(T_t)\}$ (note that both the number of vertices in the i-th row and $N(T_t)$ are independent of t by the isomporhism), and write*

$$U(T_1, T_2, \dots, T_\ell) = \sum_{i=1}^{k+1} \sum_{j=1}^{q(i)} f(P_1(i,j)) f(P_2(i,j)) \dots f(P_\ell(i,j))$$
$$= \sum_{n=1}^{N(T_t)} f(Q_{1,n}) f(Q_{2,n}) \dots f(Q_{\ell,n}).$$

Then

$$\overline{C}_{k,\ell}(f,T) = \max_{T_1,T_2,\ldots,T_\ell} |U(T_1,T_2,\ldots,T_\ell)|$$

where the maximum is taken over all ℓ-tuples $T_1, T_2, \ldots, T_\ell$ of proper subtrees of the type described above.

Definition 7. *The* universal correlation measure of order ℓ *of f over T is defined by*

$$\tilde{C}_\ell(f,T) = \max_k \overline{C}_{k,\ell}(f,T).$$

Definition 8. *The* normality measure $\overline{N}_k(f,T)$ of order k *($k \in \mathbb{N},\ k \geq 2$) of the binary function f over the r-almost s-uniform tree is defined in the following way: Let $\mathcal{T}_k$ denote the set of uniform binary subtrees of height k of T. If $G_{2^{k+1}-1} = (g_1, g_2, \ldots, g_{2^{k+1}-1}) \in \{-1,+1\}^{2^{k+1}-1}$, then let $\phi(f,T,G_{2^{k+1}-1})$ denote the number of the subtrees $T' \in \mathcal{T}_k$ such that the binary sequence $E_{2^{k+1}-1} = E_{2^{k+1}-1}(f,T')$ assigned to the binary function $f:\ \mathcal{V}(T') \to \{-1,+1\}$ (i.e., f restricted to T') is the given $2^{k+1}-1$ tuple $G_{2^{k+1}-1}$:*

$$\phi(f,T,G_{2^{k+1}-1}) = \left|\{T':\ T' \in \mathcal{T}_k,\ E_{2^{k+1}-1}(f,T') = G_{2^{k+1}-1}\}\right|.$$

Then define $\overline{N}_k(f,T)$ by

$$\overline{N}_k(f,T) = \max_{G_{2^{k+!}-1} \in \{-1,+1\}^{2^{k+1}-1}} \left|\phi(f,T,G_{2^{k+1}-1}) - \frac{|\mathcal{T}_k|}{2^{2^{k+1}-1}}\right|.$$

(So that $\overline{N}_k(f,T)$ is defined as the maximal deviation between $\phi(f,T,G_{2^{k+1}-1})$ and its expected value of all the possible choices of $G_{2^{k+1}-1}$.)

4. The measures of pseudorandomness of binary functions on general trees.

The definition of the well-distribution measure in Definition 5 can be used in case of general trees as well.

The definitions of the correlation measure and universal correlation measure in Definitions 6 and 7 also can be used for general trees; note that the notion of proper subtree occurring in Definition 6 is defined here in a slightly different way as in [4]. However, in case of general trees there is another, much greater problem. Namely, if the degree of the vertices are large, then it may occur that there are very few isomorphic pairs of proper subtrees. Even it may occur that there are no pairs of vertices of the same (positive) degree,

and then there are no isomorphic proper subtrees (of at least two vertices) at all so that the definition of correlation becomes empty.

To help on this problem we may introduce further correlation measures. One way to do this is to use the "correlation analogue" of Definition 5:

Definition 9. *The* horizontal correlation measure of order k *of the binary function* f *over* T *is defined by*

$$\overline{C}'_k(f,T) = C_k(E_N(f,T)).$$

(The use of the adjective "horizontal" will be explained later.) To extend the notion of normality measure to general trees is even more troublesome. First, one might like to replace the binary subtrees in Definition 8 by proper subtrees. Then again it can be a problem that it may occur that there are no isomorphic subtrees. We have been trying to introduce a normality measure in the manner of Definitions 5 and 9 but we have not been able to find a reasonable definition. Thus in the case of general trees we will not define normality measure.

Since some of the measures of pseudorandomness defined in [4] cannot be extended to general trees or the extended measures have only a limited use, thus we have to look for new measures. Our starting point can be that when we introduce quantitative measures of pseudorandomness in different structures then these measures are related to some sort of ordering. In case of rooted plane trees there are two natural ways to order the vertices: the vertices at any fixed level possess a from-left-to-right order, and the vertices along a path starting with the root and ending with a leaf can be ordered according to their distance from the root. We will refer to these orderings as *horizontal* resp. *vertical ordering*. Definitions 5 and 9 are related to the horizontal ordering, and the discussion in [4] shows that in the measures in Definitions 6 and 7 also the horizontal ordering plays a dominant role. Thus the new measures to be introduced have to be related to the *vertical* ordering of the tree.

Let $\mathbb{P}$ denote the set of the paths starting from the root and ending at the last level (note that now we are considering regular trees so that every other path is a part of a path belonging to $\mathbb{P}$), and for a path $\mathcal{P} \in \mathbb{P}$ let $V_0(\mathcal{P})$, $V_1(\mathcal{P}), \dots, V_h(\mathcal{P})$ be the vertices of $\mathcal{P}$ (so that $V_i(\mathcal{P})$ is the vertex at level i) and define the binary sequence $G(\mathcal{P})$ by

$$G(\mathcal{P}) = (g_1(\mathcal{P}), g_2(\mathcal{P}), \dots, g_{h+1}(\mathcal{P})) = (f(V_0(\mathcal{P})), f(V_1(\mathcal{P})), \dots, f(V_h(\mathcal{P}))).$$

Definition 10. *The* strong vertical well-distribution measure *of the binary function* $f : T \to$

$\{-1,+1\}$ *is defined by*

$$SW(f,T) = \max_{\mathcal{P}\in\mathbb{P}} W(G(\mathcal{P})).$$

Definition 11. *For* $k \in \mathbb{N},\ k \geq 2$ *the* strong vertical correlation measure of order k *of the binary function* $f:\ T \to \{-1,+1\}$ *is defined by*

$$SC_k(f,T) = \max_{\mathcal{P}\in\mathbb{P}} C_k(G(\mathcal{P})).$$

When we introduce a new measure for pseudorandomness of binary functions then it is a basic requirement that for a truly random binary function the measure of it should be much much smaller than the maximum of it over all binary functions (attained usually when the function is identically $+1$); more precisely, their quotient must have limit 0 as $N(T) \to \infty$. Namely, if this requirement holds then we may consider as a good pseudorandom property of the given function if its measure is small. In case of the measures introduced in the last two definitions this requirement does not always hold.

Example 1. Let $H \in \mathbb{N}$, $H \to \infty$ and consider the 4-uniform tree T of height $h = 2H$. Then it is easy to see that for almost all binary function $f:\ T \to \{-1,+1\}$ there is a path $\mathcal{P} \in \mathbb{P}$ such that

$$\begin{aligned} G(\mathcal{P}) &= (g_1(\mathcal{P}), g_2(\mathcal{P}), \ldots, g_{2H+1}(\mathcal{P})) \\ &= (f(V_0(\mathcal{P})), f(V_1(\mathcal{P})), \ldots, f(V_{2H}(\mathcal{P})) \\ &= (f(V_0(\mathcal{P})), f(V_1(\mathcal{P})), \ldots, f(V_{H+1}(\mathcal{P}), 1, 1, \ldots, 1) \end{aligned}$$

so that both $SW(f,T)$ and $SC_k(f,T)$ are large:

$$SW(f,T) = W(G,\mathcal{P}) = \sum_{i=H+1}^{2H} 1 = H = \frac{h}{2}$$

and

$$SC_k(f,T) = C_k(G,\mathcal{P}) = \sum_{i=H+1}^{2H+1-k} 1 = H + 1 - k = \frac{h}{2} + 1 - k.$$

In order to handle this situation we have to introduce further (weaker) measures. These measures can be defined by taking average instead of maximum in Definitions 10 and 11. This average taking can be done in two ways: we may take the average of $W(G(\mathcal{P}))$, resp. $C_k(G(\mathcal{P}))$ over all $\mathcal{P} \in \mathbb{P}$, or we may take the average of the absolute values of all the sums whose maximum gives the value of $W(G(\mathcal{P}))$, resp. $C_k(G(\mathcal{P}))$.

Definition 12. *The* weak vertical well-distribution measure of first type *of the binary function* $f: T \to \{-1,+1\}$ *is defined by*

$$A_1W(f,T) = \frac{1}{|\mathcal{P}|}\sum_{\mathcal{P}\in\mathbb{P}} W(G(\mathcal{P})).$$

Definition 13. *The* weak vertical correlation measure of order k of first type *of the binary function* $f: T \to \{-1,+1\}$ *is defined by*

$$A_1C_k(f,T) = \frac{1}{|\mathcal{P}|}\sum_{\mathcal{P}\in\mathbb{P}} C_k(G(\mathcal{P})).$$

Definition 14. *The* weak vertical well-distribution measure of second type *of the binary function* $f: T \to \{-1,+1\}$ *is defined by*

$$A_2W(f,T) = \frac{\sum_{(a,b,t):\ 1\le a\le a+(t-1)b\le h+1}\sum_{\mathcal{P}\in\mathbb{P}}\left|\sum_{j=0}^{t-1} g_{a+jb}(\mathcal{P})\right|}{\sum_{\mathcal{P}\in\mathbb{P}}\sum_{(a,b,t):\ 1\le a\le a+(t-1)b\le h+1} 1}$$

which can be rewritten as

$$A_2W(f,T) = \frac{\sum_{\mathcal{P}\in\mathbb{P}}\sum_{(a,b,t):\ 1\le a\le a+(t-1)b\le h+1}\left|\sum_{j=0}^{t-1} g_{a+jb}(\mathcal{P})\right|}{|\mathbb{P}|\sum_{(a,b,t):\ 1\le a\le a+(t-1)b\le h+1} 1}.$$

Definition 15. *The* weak vertical correlation measure of order k of the second type *of the binary function* $f: T \to \{-1,+1\}$ *is defined by*

$$A_2C_k(f,T) = \frac{\displaystyle\sum_{\mathcal{P}\in\mathbb{P}}\sum_{M=1}^{h+1-k}\sum_{0\le d_1<d_2<\cdots<d_k\le h+1-M}\left|\sum_{n=1}^{M} g_{n+d_1}(\mathcal{P})g_{n+d_2}(\mathcal{P})\dots g_{n+d_k}(\mathcal{P})\right|}{|\mathbb{P}|\displaystyle\sum_{M=1}^{h+1-k}\sum_{0\le d_1<d_2<\cdots<d_k\le h+1-M} 1}.$$

We will illustrate the different role of the strong and weak vertical measures by an example.

Example 2. Let p be a large prime number, and let T denote the 2-uniform binary tree of height $p-2$. Define the binary function $f_1: T \to \{-1,+1\}$ so that for $i = 1,2,\dots,p-1$, at each vertex in the i-th row it assumes the value $\left(\frac{i}{p}\right)$:

$$f_1(P_T(i,1)) = f_1(P_T(i,2)) = \cdots = f_1(P_T(i,2^{i-1})) = \left(\frac{i}{p}\right).$$

Then for every path $\mathcal{P} \in \mathbb{P}$ the binary sequence $G(\mathcal{P})$ assigned to $\mathcal{P}$ is

$$\begin{aligned} G(\mathcal{P}) &= (g_1(\mathcal{P}), g_2(\mathcal{P}), \ldots, g_{p-1}(\mathcal{P})) \\ &= (f_1(V_0(\mathcal{P})), f_1(V_1(\mathcal{P})), \ldots, f_1(V_{p-2}(\mathcal{P}))) \\ &= \left(\left(\frac{1}{p}\right), \left(\frac{2}{p}\right), \ldots, \left(\frac{p-1}{p}\right) \right). \end{aligned}$$

It is known [6] that for this Legendre symbol sequence both W and C_k (for fixed k) measures are "small" (less than $p^{1/2}(\log p)^c$). It follows that each of the vertical measures in Definitions 10-15 is also small.

Now we modify this function f_1 so that we consider the path $\mathcal{P}_0$ which connects the first vertices of the rows, and then we change the function f_1 on the second half of the vertices in $\mathcal{P}_0$ for $+1$, so that denoting the new function by f_2 we have

$$f_2(V_i(\mathcal{P}_0) = +1) \quad \text{for} \quad i = \frac{p-1}{2}, \frac{p+1}{2}, \ldots, p-2, \tag{4..1}$$

and at every other vertex $V_i(\mathcal{P})$ with $V_i(\mathcal{P}) \notin \{V_{\frac{p-1}{2}}(\mathcal{P}_0), V_{\frac{p+1}{2}}(\mathcal{P}_0), \ldots, V_{p-2}(\mathcal{P}_0)\}$ we have

$$f_1(V_i(\mathcal{P})) = f_2(V_i(\mathcal{P})).$$

Then we have

$$G(\mathcal{P}_0) = \left(\left(\frac{1}{p}\right), \left(\frac{2}{p}\right), \ldots, \left(\frac{\frac{p-1}{2}}{p}\right), +1, +1, \ldots, +1 \right),$$

and the last +1's make both $W(G(\mathcal{P}_0))$ and $C_k(G(\mathcal{P}_0))$ (for fixed k) large (as in Example 1) thus each of the strong measures in Definitions 10 and 11 is also large for f_2. On the other hand, there are only "very few" paths $\mathcal{P} \in \mathbb{P}$ which contain one of the vertices $V_i(\mathcal{P}_0)$ appearing in (4..1), and thus their contribution to the averages in Definitions 12-15 is negligible, so that each of the weak vertical measures is small for f_2 (just slightly greater than for f_1).

5. Measures of pseudorandomness for a truly random binary function defined on a given tree.

As we said in Section 4 a new measure of pseudorandomness of binary functions must satisfy the requirement that for a truly random binary function the measure of it is much

smaller, than the maximum of it over all binary functions defined on the given tree. It follows from the results in [2] and [4] that this is so in case of the measures defined in Definitions 5-9. It remains to show that the vertical measures defined in Definitions 12-15 also possess this property (the case of Definitions 10 and 11 was discussed in Section 4). This could be proved by adapting the moment method used in [2]. Since the proofs would be similar, thus here we restrict ourselves to the case of Definition 15 (the case of Definition 13 would be slightly more difficult while the remaining two cases would be slightly easier).

Theorem 1. *Let $k \in \mathbb{N}$, and let T be a regular rooted plane tree of height h. Choose the binary function $f : \mathcal{V}(= \mathcal{V}(T)) \to \{-1, +1\}$ in random way, i.e., choose these binary functions independently and with equal probability $\frac{1}{2^{|\mathcal{V}|}}$. If h is large in terms of k then for all $0 < \varepsilon < 1$ we have*

$$P\left(A_2 C_k(f,T)) > \frac{11}{\varepsilon}(k(h+1)\log(h+1))^{1/2}\right) < \varepsilon. \tag{5..1}$$

(So that for fixed k and $h \to \infty$ we have $A_2 C_k(f,T) = O\left((h\log h)^{1/2}\right)$ with large probability.) We remark that while we will prove this *upper* bound by using the moment method which can be adapted relatively easily in the most cases, it seems much more difficult, perhaps, hopeless to adapt the more sophisticated methods used in [1] and [5] for giving a probabilistic *lower* bound.

Proof of Theorem 1. We will reduce the problem to the case of random *binary sequences* studied first in [2] (and later in [1] and [5]). First we will prove

Lemma 1. *For every $k \in \mathbb{N}$ there is a number $H_0 = H_0(k)$ such that if $H \in \mathbb{N}$ and $H > H_0$ then*

$$S = \sum_{G_H=\{g_1,\dots,g_H\}\in\{-1,+1\}^H} \sum_{M=1}^{H-k} \sum_{0\le d_1<\dots<d_k\le H-M} \left|\sum_{n=1}^{M} g_{n+d_1}\cdots g_{n+d_k}\right|$$
$$< 11(kH\log H)^{1/2} 2^H \sum_{M=1}^{H-k} \sum_{0\le d_1<\dots<d_k\le H-M} 1. \tag{5..2}$$

Proof of Lemma 1. We will adapt the method used in [2]. Indeed, as in [2], we start out from the sum

$$S_{H,k}(\ell) = \sum_{G_H=\{g_1,\dots,g_H\}\in\{-1,+1\}^H} \sum_{M} \sum_{D} \left|\sum_{n=1}^{M} g_{n+d_1}\cdots g_{n+d_k}\right|^{2\ell}$$

which (apart from notation) appears in [2] in (2.21), where the inner sums are taken over all $M \in \mathbb{N}$, $D = (d_1, \ldots, d_k)$ with $0 \le d_1 < \cdots < d_k$ and $M + d_k \le H$, and $\ell \in \mathbb{N}$ is fixed later in (2.28) as

$$\ell = [2k \log H]. \tag{5..3}$$

However, up to (2.32) only $\ell = o(M)$ is used for $H^{1/4} < M \le H$ so that up to this point it suffices to assume that

$$\ell = o(H^{1/4}). \tag{5..4}$$

In other words, if (5..4) is assumed then (2.32) in [2] holds:

$$S_{H,k}(\ell) < 5 \cdot 2^H H^{k+\ell+2} (4\ell)^\ell. \tag{5..5}$$

Now we take a slightly greater ℓ than the one in (5..3): we fix ℓ as

$$\ell = [3k \log H] \tag{5..6}$$

so that (5..4) holds trivially (if H is large enough in terms of k). We split the sum S in two parts: let S' denote the sum of terms with

$$\left| \sum_{n=1}^{M} g_{n+d_1} \cdots g_{n+d_k} \right| < 10(kH \log H)^{1/2} \tag{5..7}$$

and let S" denote the sum of terms for that the opposite inequality holds. Then clearly we have

$$\begin{aligned} S' &< \sum_{G_H \in \{-1,+1\}^H} \sum_{M} \sum_{D} 10(kH \log H)^{1/2} \\ &= 10(kH \log H)^{1/2} 2^H \sum_{M=1}^{H-k} \sum_{0 \le d_1 < \cdots < d_k \le H-M} 1. \end{aligned} \tag{5..8}$$

Let X denote the number of terms in S", i.e., the number of terms for which the opposite of (5..7) holds. Keeping only these terms in the sum $S_{H,k}(\ell)$ we get

$$S_{H,k}(\ell) \ge X \left(10(kH \log H)^{1/2} \right)^{2\ell} = X \left(100kH \log H \right)^{\ell}. \tag{5..9}$$

By (5..6), it follows from (5..5) and (5..9) for H large enough that

$$\begin{aligned} X &< 5 \cdot 2^H H^{k+2} (\ell/(25kH \log H))^\ell < 5 \cdot 2^H H^{k+2} 8^{-3k \log H} \\ &< 5 \cdot 2^H H^{k+2} H^{-6k} = 5 \cdot 2^H H^{-5k+2}. \end{aligned} \tag{5..10}$$

A trivial upper bound for the left hand side of (5..7) is $M \le H$. Thus by (5..10) and the definition of S" and X we have

$$S" \le XH < 5 \cdot 2^H H^{-5k+3} < 2^H \tag{5..11}$$

for H large enough. (5..2) follows from (5..8) and (5..11) and this completes the proof of the lemma.

In order to prove (5..1), we start out from the sum

$$\sum_{f:\, T\to\{-1,+1\}} A_2 C_k(f,T)$$

which, by Definition 15, can be rewritten as

$$\sum_{f:\, T\to\{-1,+1\}} A_2 C_k(f,T) = \frac{\sum_{f:\, T\to\{-1,+1\}} \sum_{\mathcal{P}\in\mathbb{P}} \sum_M \sum_D \left|\sum_{n=1}^M g_{n+d_1}(\mathcal{P})\dots g_{n+d_k}(\mathcal{P})\right|}{|\mathbb{P}| \sum_M \sum_D 1} \tag{5..12}$$

where M and D run over all $M \in \mathbb{N}$, $D = (d_1,\dots,d_k)$ with $1 \le M \le h+1-k$, $0 \le d_1 < \dots < d_k$, $M + d_k \le h+1$. If we change the order of summation and use Lemma 1 (with $h+1$ in place of H), then the numerator can be estimated in the following way for h large enough:

$$\begin{aligned}
&\sum_{f:\, T\to\{-1,+1\}} \sum_{\mathcal{P}\in\mathbb{P}} \sum_M \sum_D \left|\sum_{n=1}^M g_{n+d_1}(\mathcal{P})\dots g_{n+d_k}(\mathcal{P})\right| \\
&= \sum_{\mathcal{P}\in\mathbb{P}} \sum_{f:\, (\mathcal{V}\setminus\{V_0(\mathcal{P}),\dots,V_h(\mathcal{P})\})\to\{-1,+1\}} \sum_{G_{h+1}=\{g_1,\dots,g_{h+1}\}\in\{-1,+1\}^{h+1}} \sum_M \sum_D \\
&\qquad\qquad \left|\sum_{n=1}^M g_{n+d_1}\dots g_{n+d_k}\right| \\
&= \sum_{\mathcal{P}\in\mathbb{P}} 2^{|\mathcal{V}|-(h+1)} \sum_{G_{h+1}=\{g_1,\dots,g_{h+1}\}\in\{-1,+1\}^{h+1}} \sum_M \sum_D \\
&\qquad\qquad \left|\sum_{n=1}^M g_{n+d_1}\dots g_{n+d_k}\right| \\
&< \sum_{\mathcal{P}\in\mathbb{P}} 2^{|\mathcal{V}|-(h+1)} \cdot 11\,(k(h+1)\log(h+1))^{1/2}\, 2^{h+1} \sum_M \sum_D 1 \\
&= 11\,(k(h+1)\log(h+1))^{1/2}\, 2^{|\mathcal{V}|}\, |\mathbb{P}| \sum_M \sum_D 1.
\end{aligned} \tag{5..13}$$

It follows from (5..12) and (5..13) that

$$\sum_{f\colon T\to\{-1,+1\}} A_2C_k(f,T) < 11\left(k(h+1)\log(h+1)\right)^{1/2}2^{|\mathcal{V}|}. \tag{5..14}$$

Clearly we have

$$\begin{aligned}&\sum_{f\colon T\to\{-1,+1\}} A_2C_k(f,T) \geq \\ &\left|\{f:\ T\to\{-1,+1\}, A_2C_k(f,T) > \frac{11}{\varepsilon}\left(k(h+1)\log(h+1)\right)^{1/2}\}\right| \cdot \\ &\cdot \frac{11}{\varepsilon}\left(k(h+1)\log(h+1)\right)^{1/2}.\end{aligned} \tag{5..15}$$

It follows from (5..14) and (5..15) that

$$\begin{aligned}&P\left(A_2C_k(f,T) > \frac{11}{\varepsilon}\left(k(h+1)\log(h+1)\right)^{1/2}\right) \\ &= \left|\{f:\ T\to\{-1,+1\}, A_2C_k(f,T) > \frac{11}{\varepsilon}\left(k(h+1)\log(h+1)\right)^{1/2}\}\right| \cdot \frac{1}{2^{|\mathcal{V}|}} \\ &< \varepsilon\end{aligned}$$

which completes the proof of the theorem.

6. Connection between the measures of pseudorandomness

In Definitions 5,6,7,9,10,11,12,13,14 and 15 we have proposed 10 measures of pseudorandomness. If two measures are given so that if either of them is small (in terms of the trivial estimate) then the other one also must be small, then it suffices to study one of them while the other can be discarded. Thus one might like to show that the measures in these 10 definitions are pairwise independent, i.e., for any pair of them either one of them can be large while the other one is small. We studied the connection between the measures 5,6,7 and 9 in earlier papers. It is clear that the vertical well-distribution measures and correlation measures are independent. On the other hand, the vertical measures are not quite independent: if a strong measure is small then the corresponding weak measures are also small. In spite of this we also need the weak measures as Example 1 and the discussion after it shows.

It remains to study the connection between the horizontal and vertical ones. In the rest of this section we will show by examples that the horizontal measures are independent of the vertical ones.

Example 3. Consider the following generalization of the binary function defined in Example 2: let T be any regular rooted plane tree of height $h = p - 2$ where p is a large prime number, and define the binary function f on T so that for every vertex $P(i,j)$ at level i we have $f(P(i,j)) = \left(\frac{i}{p}\right)$. Then for every path $\mathcal{P} \in \mathbb{P}$ we have

$$G(\mathcal{P}) = (g_1(\mathcal{P}), g_2(\mathcal{P}), \dots, g_{h+1}(\mathcal{P})) = \left(\left(\frac{1}{p}\right), \left(\frac{2}{p}\right), \dots, \left(\frac{p-1}{p}\right)\right),$$

thus clearly it follows from the results on this Legendre symbol sequence in [6] that all the vertical measures in Definitions 10-15 are small ($< cp^{1/2}\log p$ where, in case of the correlation measures, c depends on the order of the correlation). On the other hand, if the degrees of the vertices of T are large so that at least half of the vertices belong to the last level (e.g., this is the case if the degree of every vertex is at least 2) then clearly the horizontal measures in Definitions 5 and 9 are large ($> cN$). Moreover, if there are large proper isomorphic trees in T (e.g., this is so in case of s-uniform trees with $s \geq 2$) then the correlation measures in Definitions 6 and 7 are also large. We may conclude that it may occur that all the vertical measures are small and all the other measures are large

Example 4. Let h be a large positive integer, and let p be a prime large enough in terms of h, say, let $p > h^3$. Consider the tree T which at each level $0, 1, \dots, h-1$ has a single vertex of degree 1, and at level h it has a single vertex of degree $p-1$ (see Figure 3).

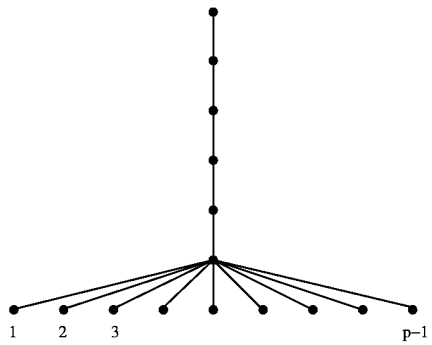

Figure 3.

Independence of the vertical and horizontal measures

Define $f : \mathcal{V}(T) \to \{-1, +1\}$ so that it assumes the value $+1$ at each of the vertices at level $0, 1, \dots, h-1$, and, moving from the left to the right, it assumes the values $\left(\frac{1}{p}\right), \left(\frac{2}{p}\right), \dots, \left(\frac{p-1}{p}\right)$ at the vertices at the last level. Then clearly all the vertical measures in Definitions 10-15 are large. On the other hand, again it follows from the results

in [6] that the horizontal measures in Definitions 5 and 9 are small. Finally, there are no pairs of proper isomorphic subtrees with more than h vertices, thus the correlation measures in Definitions 6 and 7 are small so that here the situation is just the opposite of the one in Example 3 so that, indeed, the vertical measures and the measures in Definitions 5,6,7,9 are independent.

7. Finding a binary function with strong pseudorandom properties on an arbitrary tree.

One might like to find a construction method which produces a binary function with strong pseudorandom properties on an arbitrary regular rooted planar tree. This seems to be a too ambitious task; we have seen that regular rooted planar trees can be of very different structure, and this fact leads to serious difficulties. However, we will be able to construct many "not very large " families of binary functions over any regular rooted planar tree such that each of these families contains at least one binary function with strong pseudorandom properties, so that we may search for a "good" binary function with strong pseudorandom properties in a relatively small family.

Let T be any regular tree of h levels and N vertices. Let $N < p < 2N$ be a prime number. The root of T is denoted by Q_1, the vertices in the second row are $Q_2, Q_3, \dots, Q_{y_2+1}$, the vertices in the third row are $Q_{y_2+2}, Q_{y_2+3}, \dots, Q_{y_2+y_3+1}$ and so on; finally Q_N is the last vertex in the last row.

Let $g(x) \in \mathbb{F}_p[x]$ be an irreducible polynomial of degree $r \geq 2$. For $0 \leq x < p$ we define a binary function f_x on this tree T in the following way:

$$f_x(Q_n) = \left(\frac{g(x+n)}{p} \right).$$

We will prove:

Theorem 2. *For all $x \in \mathbb{F}_p$ we have*

$$\overline{W}(f_x, T) \ll rN^{1/2} \log N. \tag{7..1}$$

For every $L < N$ there exists an $x \in \mathbb{F}_p$ such that

$$A_2 W(f_x, T) \ll \frac{hLr^{1/2}}{N^{1/4}} + h^{1/2} L^{1/2} \tag{7..2}$$

and for $2 \le \ell \le L$

$$A_2 C_\ell(f_x, T) \ll \frac{hLr^{1/2}}{N^{1/4}} + h^{1/2}L^{1/2}. \tag{7..3}$$

If $Lhr \ll N^{1/2}$ then as a corollary we get:

Corollary 1. *For every* $L \le \frac{N^{1/2}}{hr}$ *there exists an* $x \in \mathbb{F}_p$ *such that*

$$A_2 W(f_x, T) \ll h^{1/2}L^{1/2}$$

and for $2 \le \ell \le L$

$$A_2 C_\ell(f_x, T) \ll h^{1/2}L^{1/2}.$$

Proof of Theorem 2.

First we will prove (7..1).

$$\begin{aligned}
\overline{W}(f_x, T) &= W(E_N(f_x, T)) \\
&= W\left(\left\{\left(\frac{g(x+1)}{p}\right), \left(\frac{g(x+2)}{p}\right), \dots, \left(\frac{g(x+N)}{p}\right)\right\}\right) \\
&\le W\left(\left\{\left(\frac{g(x+1)}{p}\right), \left(\frac{g(x+2)}{p}\right), \dots, \left(\frac{g(x+p)}{p}\right)\right\}\right) \\
&= \max_{a,b,t} \left|\sum_{j=0}^{t-1} \left(\frac{g(x+a+jb)}{p}\right)\right|
\end{aligned} \tag{7..4}$$

where the maximum is taken over all $a, b, t \in \mathbb{N}$ with $1 \le a \le a + (t-1)b \le p$. We will use:

Lemma 2. *Suppose that* p *is a prime,* χ *is a non-principal character modulo* p *of order* d*,* $f \in \mathbb{F}_p[x]$ *has* s *distinct roots in* $\overline{\mathbb{F}}_p$*, and it is not a constant multiple of the* d*-th power of a polynomial over* $\mathbb{F}_p$*. Then:*

$$\left|\sum_{n \in \mathbb{F}_p} \chi(f(n))\right| < sp^{1/2}.$$

Poof of Lemma 2.

This is a special case of Weil's theorem [9] (see also [7]). Next we state the incomplete version of Lemma 2:

Lemma 3. *Suppose that* p *is a prime,* χ *is a non-principal character modulo* p *of order* d*,* $f \in \mathbb{F}_p[x]$ *has* s *distinct roots in* $\overline{\mathbb{F}}_p$*, and it is not a constant multiple of the* d*-th power of a polynomial over* $\mathbb{F}_p$*. Let* y *be a real number with* $0 < y \le p$*. Then for any* $x \in \mathbb{R}$*:*

$$\left|\sum_{x < n \le x+y} \chi(f(n))\right| < 9sp^{1/2}\log p.$$

Poof of Lemma 3.

This follows from Lemma 2 (see e.g. [6]).

Using Lemma 3 and (7..4) we get

$$\overline{W}(f_x, T) \ll rp^{1/2} \log p \ll rN^{1/2} \log N,$$

which was to be proved.

Next we prove (7..2) and (7..3). Indeed we will prove:

$$\frac{1}{p} \sum_{x \in \mathbb{F}_p} \left((A_2 W(f_x, T))^2 + \sum_{2 \le \ell \le L} (A_2 C_\ell(f_x, T))^2 \right) \ll \frac{h^2 L^2 r}{N^{1/2}} + hL. \tag{7..5}$$

From (7..5) it follows that (7..2) and (7..3) hold, since the average of p different positive numbers is greater than or equal to the minimum of these numbers. Thus there exists an x for which

$$(A_2 W(f_x, T))^2 + \sum_{2 \le \ell \le L} (A_2 C_\ell(f_x, T))^2 \ll \frac{h^2 L^2 r}{N^{1/2}} + hL$$

from which (7..2) and (7..3) follows. Thus we need to prove (7..5). In order to do so we will estimate

$$B_1 \stackrel{\text{def}}{=} \frac{1}{p} \sum_{x \in \mathbb{F}_p} (A_2 W(f_x, T))^2$$

and for $2 \le \ell \le L$

$$B_\ell \stackrel{\text{def}}{=} \frac{1}{p} \sum_{x \in \mathbb{F}_p} (C_\ell(f_x, T))^2 .$$

Clearly,

$$\frac{1}{p} \sum_{x \in \mathbb{F}_p} \left((A_2 W(f_x, T))^2 + \sum_{2 \le \ell \le L} (A_2 C_\ell(f_x, T))^2 \right) = B_1 + \sum_{2 \le \ell \le L} B_\ell. \tag{7..6}$$

First we estimate B_1:

$$\begin{aligned} B_1 &= \frac{1}{p} \sum_{x \in \mathbb{F}_p} (A_2 W(f_x, T))^2 \\ &= \frac{1}{p} \frac{\sum\limits_{x \in \mathbb{F}_p} \left(\sum\limits_{\mathcal{P} \in \mathbb{P}} \sum\limits_{(a,b,t):\ 1 \le a+(t-1)b \le h+1} \left| \sum\limits_{j=0}^{t-1} f_x(V_{a+jb-1}(\mathcal{P})) \right| \right)^2}{\left(\sum\limits_{\mathcal{P} \in \mathbb{P}} \sum\limits_{(a,b,t):\ 1 \le a+(t-1)b \le h+1} 1 \right)^2}. \end{aligned}$$

By the Cauchy-Schwarz inequality

$$B_1 \le \frac{1}{p}\frac{\sum\limits_{x\in\mathbb{F}_p}\sum\limits_{\mathcal{P}\in\mathbb{P}\,(a,b,t):\ 1\le a+(t-1)b\le h+1}\left(\sum\limits_{j=0}^{t-1} f_x(V_{a+jb-1}(\mathcal{P}))\right)^2}{\sum\limits_{\mathcal{P}\in\mathbb{P}\,(a,b,t):\ 1\le a+(t-1)b\le h+1}\ \sum 1}$$

$$= \frac{1}{p}\frac{\sum\limits_{\mathcal{P}\in\mathbb{P}\,(a,b,t):\ 1\le a+(t-1)b\le h+1}\ \sum\limits_{x\in\mathbb{F}_p}\sum\limits_{j_1=0}^{t-1}\sum\limits_{j_2=0}^{t-1} f_x(V_{a+j_1b-1}(\mathcal{P}))f_x(V_{a+j_2b-1}(\mathcal{P}))}{\sum\limits_{\mathcal{P}\in\mathbb{P}\,(a,b,t):\ 1\le a+(t-1)b\le h+1}\ \sum 1}. \tag{7..7}$$

For a moment fix a, b, t and the path $\mathcal{P}$. Say, $\mathcal{P}$ contains the vertices $V_0(\mathcal{P}) = Q_{c_1}, V_1(\mathcal{P}) = Q_{c_2}, \dots, V_h(\mathcal{P}) = Q_{c_{h+1}}$ (where $c_1 = 1$). Then

$$\sum_{x\in\mathbb{F}_p}\sum_{j_1=0}^{t-1}\sum_{j_2=0}^{t-1} f_x(V_{a+j_1b-1}(\mathcal{P}))f_x(V_{a+j_2b-1}(\mathcal{P}))$$

$$\sum_{x\in\mathbb{F}_p}\sum_{j_1=0}^{t-1}\sum_{j_2=0}^{t-1} f_x(Q_{c_{a+j_1b}})f_x(Q_{c_{a+j_2b}})$$

$$= \sum_{x\in\mathbb{F}_p}\sum_{j_1=0}^{t-1}\sum_{j_2=0}^{t-1}\left(\frac{g(x+c_{a+j_1b})}{p}\right)\left(\frac{g(x+c_{a+j_2b})}{p}\right)$$

$$= \sum_{0\le j_1\ne j_2\le t-1}\ \sum_{x\in\mathbb{F}_p}\left(\frac{g(x+c_{a+j_1b})g(x+c_{a+j_2b})}{p}\right) + \sum_{x\in\mathbb{F}_p}\sum_{j_1=0}^{t-1} 1.$$

Using this and Lemma 1 (note that the polynomial inside is not constant times of a square of a polynomial since the c_i's are pairwise distinct and nonzero) we get

$$\sum_{x\in\mathbb{F}_p}\sum_{j_1=0}^{t-1}\sum_{j_2=0}^{t-1} f_x(V_{a+j_1b-1}(\mathcal{P}))f_x(V_{a+j_2b-1}(\mathcal{P}))$$

$$\le t^2 2rp^{1/2} + tp \le 2(h+1)^2 rp^{1/2} + (h+1)p.$$

By this and (7..7)

$$B_1 \le \frac{1}{p}\cdot\frac{\sum\limits_{\mathcal{P}\in\mathbb{P}\,(a,b,t):\ 1\le a\le a+(t-1)b\le p}\ \sum (r(h+1)^2p^{1/2} + (h+1)p)}{\sum\limits_{\mathcal{P}\in\mathbb{P}\,(a,b,t):\ 1\le a\le a+(t-1)b\le p}\ \sum 1}$$

$$\le 2r\frac{(h+1)^2}{p^{1/2}} + (h+1). \tag{7..8}$$

Next we estimate B_ℓ:

$$B_\ell = \frac{1}{p}\sum_{x\in\mathbb{F}_p}(A_2C_\ell(f_x,T))^2$$
$$= \frac{1}{p}\sum_{x\in\mathbb{F}_p}\left(\frac{\sum\limits_{\mathcal{P}\in\mathbb{P}}\sum\limits_{M=1}^{h+1-\ell}\sum\limits_{0\le d_1<\cdots<d_\ell\le h+1-M}\left|\sum\limits_{n=1}^{M} f_x(V_{n+d_1-1}(\mathcal{P}))\dots f_x(V_{n+d_\ell-1}(\mathcal{P}))\right|}{\sum\limits_{\mathcal{P}\in\mathbb{P}}\sum\limits_{0\le d_1<\cdots<d_\ell\le h+1-M}1}\right)^2.$$

By the Cauchy-Schwarz inequality

$$B_\ell \le \frac{1}{p}\frac{\sum\limits_{x\in\mathbb{F}_p}\sum\limits_{\mathcal{P}\in\mathbb{P}}\sum\limits_{M=1}^{h+1-\ell}\sum\limits_{0\le d_1<\cdots<d_\ell\le h+1-M}\left|\sum\limits_{n=1}^{M} f_x(V_{n+d_1-1}(\mathcal{P}))\dots f_x(V_{n+d_\ell-1}(\mathcal{P}))\right|^2}{\sum\limits_{\mathcal{P}\in\mathbb{P}}\sum\limits_{M=1}^{h+1-\ell}\sum\limits_{0\le d_1<\cdots<d_\ell\le h+1-M}1}$$
$$= \frac{1}{p\sum\limits_{\mathcal{P}\in\mathbb{P}}\sum\limits_{M=1}^{h+1-\ell}\sum\limits_{0\le d_1<\cdots<d_\ell\le h+1-M}1}\Bigg(\sum_{\mathcal{P}\in\mathbb{P}}\sum_{M=1}^{h+1-\ell}\sum_{0\le d_1<\cdots<d_\ell\le h+1-M}\sum_{x\in\mathbb{F}_p}\sum_{n_1=1}^{M}\sum_{n_2=1}^{M}$$
$$f_x(V_{n_1+d_1-1}(\mathcal{P}))\dots f_x(V_{n_1+d_\ell-1}(\mathcal{P}))f_x(V_{n_2+d_1-1}(\mathcal{P}))\dots f_x(V_{n_2+d_\ell}(\mathcal{P}))\Bigg). \tag{7..9}$$

For a moment fix M, $0\le d_1<\cdots<d_\ell\le h+1-M$ and the path $\mathcal{P}$. Say, $\mathcal{P}$ contains the vertices $V_0(\mathcal{P})=Q_{c_1}, V_1(\mathcal{P})=Q_{c_2},\dots,V_h(\mathcal{P})=Q_{c_{h+1}}$ (where $c_1=1$). Then

$$\sum_{x\in\mathbb{F}_p}\sum_{n_1=1}^{M}\sum_{n_2=1}^{M}$$
$$f_x(V_{n_1+d_1-1}(\mathcal{P}))\dots f_x(V_{n_1+d_\ell-1}(\mathcal{P}))f_x(V_{n_2+d_1-1}(\mathcal{P}))\dots f_x(V_{n_2+d_\ell-1}(\mathcal{P}))$$
$$= \sum_{1\le n_1\ne n_2\le M}$$
$$\sum_{x\in\mathbb{F}_p}\left(\frac{g(x+c_{n_1+d_1})\dots g(x+c_{n_1+d_\ell})g(x+c_{n_2+d_1})\dots g(x+c_{n_2+d_\ell})}{p}\right)$$
$$+\sum_{x\in\mathbb{F}_p}\sum_{n_1=1}^{M}1.$$

Since $c_1,c_2,\dots,c_{h+1}$ are pairwise distinct the two sets $\{c_{n_1+d_i}:\ 1\le i\le\ell\}$ and $\{c_{n_2+d_i}:\ 1\le i\le\ell\}$ are the same if and only if the two sets $\{n_1+d_i:\ 1\le i\le\ell\}$ and $\{n_2+d_i:\ 1\le i\le\ell\}$ are the same, which is equivalent with $n_1=n_2$. Thus the polynomial

$g(x+c_{n_1+d_1})\dots g(x+c_{n_1+d_\ell})g(x+c_{n_2+d_1})\dots g(x+c_{n_2+d_\ell})$ is not the square of a polynomial. Thus by using Lemma 1 we obtain

$$\sum_{x\in\mathbb{F}_p}\sum_{n_1=1}^{M}\sum_{n_2=1}^{M}$$
$$f_x(V_{n_1+d_1-1}(\mathcal{P}))\dots f_x(V_{n_1+d_\ell-1}(\mathcal{P}))f_x(V_{n_2+d_1-1}(\mathcal{P}))\dots f_x(V_{n_2+d_\ell-1}(\mathcal{P}))$$
$$\le M^2 2r\ell p^{1/2}+Mp\le h^2 2r\ell p^{1/2}+hp.$$

By this and (7..9) we get

$$B_\ell\le\frac{h^2 2r\ell}{p^{1/2}}+h.$$

Using this, (7..6) and (7..8) we obtain

$$\frac{1}{p}\sum_{x\in\mathbb{F}_p}\left((A_2W(f_x,T))^2+\sum_{2\le\ell\le L}(A_2C_\ell(f_x,T))^2\right)\ll\sum_{\ell=1}^{L}\left(\frac{h^2\ell r}{p^{1/2}}+h\right)$$
$$\ll\frac{h^2L^2r}{p^{1/2}}+hL$$
$$\ll\frac{h^2L^2r}{N^{1/2}}+hL$$

which proves (7..5).

References

[1] N. Alon, Y. Kohayakawa, C. Mauduit, C. G. Moreira and V. Rödl, *Measures of pseudorandomness for finite sequences: typical values*, Proc. London Math. Soc. 95 (2007), 778-812.

[2] J. Cassaigne, C. Mauduit and A. Sárközy, *On finite pseudorandom binary sequences VII: The measures of pseudorandomness*, Acta Arith. 103 (2002), 97-118.

[3] M. Drmota, *Random Trees*, An Interplay between Combinatorics and Probability, Springer 2009.

[4] K. Gyarmati, P. Hubert and A. Sárközy, *Pseudorandom binary functions on almost uniform trees*, J. Combin. Number Th. 2 (2010), 1-24.

[5] Y. Kohayakawa, C. Mauduit, C. G. Moreira and V. Rödl, *Measures of pseudorandomness for finite sequences: minimum and typical values*, Proceedings of WORDS'03, 159-169, TUCS Gen. Publ. 27, Turku Cent. Comput. Sci., Turku, 2003.

[6] C. Mauduit and A. Sárközy, *On finite pseudorandom binary sequences I: Measure of pseudorandomness, the Legendre symbol*, Acta Arith. 82 (1997), 365-377.

[7] W. M. Schmidt, *Equations over Finite Fields:* An Elementary Approach, Lecture Notes in Math. 536, Springer, Berlin, 1976.

[8] J.-P. Serre, *Trees*, Springer Monographs in Math., 2nd ed., Springer, Berlin, 2003.

[9] A. Weil, *Sur les courbes algébriques et les variétés qui s'en déduisent*, Act. Sci. Ind. 1041, Hermann, Paris, 1948.