Recognizing group languages with OBDDs

Ch. Choffrut[*], Y. Haddad
LIAFA, UMR 7089, Université Paris 7
2 Pl. Jussieu, Paris Cedex 75251
France

October 5, 2006

1 Introduction

Our purpose is to initiate the study of the family of recognizable languages through the use of ordered binary decision diagrams, OBDD, introduced by Bryant in [1], after C. Y. Lee, [3]. Consider an arbitrary, not necessarily recognizable, subset X of a free finitely generated monoid Σ^*. For each integer $n \geq 0$ denote by X_n the finite set of elements in X of length n and choose a permutation π_n of the set $\{1, \ldots, n\}$. An OBDD is a variant of a finite deterministic automaton which recognizes X_n in the following way. Instead of reading an input from left to right, read the letters in the order determined by the permutation π: the input is recognized if the computation leads to an accepting state otherwise it is rejected. The notion of reduced automata carries over to these new structures. For a fixed sequence of permutations $(\pi_n)_{n>0}$ we obtain a function which assigns to each integer n the size of the minimum OBDD recognizing X_n. We investigate the asymptotic behavior of these functions for all possible sequences.

One of the main issues of OBDDs is the choice of an ordering of the variables for each integer n, minimizing the size of the diagram. Wegener proposed in [5] a classification of the asymptotic sensitivity of the growth of the OBDD size relative to the choice of the variable ordering, into various families of functions. E.g., *nice* functions are those for which all variable orderings lead to polynomial OBDD size, while *very ugly* functions are those for which all variable orderings lead to exponential OBDD size. *Almost ugly*

[*]email: `cc@liafa.jussieu.fr`

functions are inbetween, in the sense that there is a way of choosing an ordering for which the growth is polynomial, but almost surely, an arbitrary choice of the variables leads to a nonpolynomial growth.

Our main result is a bit technical, so we state it under more amenable conditions. Consider a language X which is the inverse morphic image of the identity of a finite non-abelian two-generator groups where the orders of the generators are co-prime. Under the uniform distribution hypothesis over orderings on the first n integers, with probability 1 when n tends to infinity, the size of the reduced OBDD computing X_n grows at least as fast as α^n for some $\alpha > 1$. Furthermore, we show that this is not a property of the group but rather of a presentation, i.e, it depends on the way it is generated. Finally, we give sufficient conditions for the growth to be polynomial. A complete characterization of the group presentations for which the growth is non-polynomial seems still to be an open problem.

2 Preliminaries

We recall the main basic notions to make our work as self-contained as possible. We refer to Ingo Wegener's handbook for a deepening of the topic, [5].

2.1 Ordered binary decision diagram (OBDD)

We are concerned with Boolean functions $f : \{0,1\}^n \to \{0,1\}$ where the integer n is the *arity* of the function. Given a subset of indices $\{i_1, \ldots, i_k\} \subseteq \{1, \ldots, n\}$ and Boolean values $a_{i_1}, \ldots, a_{i_k}$, we consider the assignment $v : \{x_{i_1}, \ldots, x_{i_k}\} \to \{0,1\}$ defined by $v(x_{i_1}) = a_{i_1}, \ldots, v(x_{i_k}) = a_{i_k}$. We denote by $f_{|x_{i_1}=a_{i_1} \ldots, x_{i_k}=a_{i_k}} : \{0,1\}^{n-k} \to \{0,1\}$ or simply by $f_{|v}$, the *restriction* of f, i.e., the function obtained by fixing each x_{i_j} to the value a_{i_j}, for $1 \leq j \leq k$ and leaving the $n-k$ remaining variables take on arbitrary Boolean values. Such a function is also called a *subfunction* of f.

We assume the Boolean variables are taken from an infinite set $X = \{x_1, x_2, \ldots\}$. For a fixed n, an *ordering* of the variables $x_1, x_2, \ldots, x_n$ is a permutation π on the set $\{1, 2, \ldots, n\}$, i.e., an element of the symmetric group $\mathfrak{S}_n$. We now define the notion of ordered OBDD. We encourage the reader to have in mind a representation of a finite automaton for recognizing binary words of the same length, but where all letters are read in a predefined ordering, see figure 1. A π-*ordered binary decision diagram*, or π-OBDD, over a set of n Boolean variables $x_1, \ldots, x_n$, is a pair consisting of a permutation $\pi \in \mathfrak{S}_n$ and a directed acyclic graph. This graph has two nodes of outdegree 0, called the *sinks* and a specific node with indegree 0 called the *source*. All other nodes are *internal nodes* and have in-degree different from 0 and out-degree equal to 2. The nodes are labelled by one of the n variables except the two sinks which are labeled by the Boolean constants 0 and 1. The edges of the graph are labeled by the two Boolean values 0 and 1 and are called the 0- and the 1-edges respectively. Furthermore it is assumed that along a path from the source to one of the sinks, the variables are visited in the order determined by the permutation π which means that the graph can be decomposed in n levels where level 1 corresponds to the variable $x_{\pi(1)}$ and more generally, level i to the variable $x_{\pi(i)}$. The Boolean function f associated with the OBDD is now explained. Given an assignment for the Boolean variables, start up from the source and follow the unique path by taking for each node labeled by, say x_i, the outgoing edge labeled by the value of the variable in the assignment. If the path ends up in the sink 0, then f takes on the value 0, else the value 1. We say that the OBDD *computes* the Boolean function.

Example 1. Consider the function $f(x_1, x_2, x_3, x_4)$ with value 1 if and only if for some integer $1 \leq i < 4$ the equalities $x_i = 0$ and $x_{i+1} = 1$ hold. Considering the permutation π reduced to the cycle (124), consists of querying the variables in the order x_2, x_4, x_3 and x_1 and leads to the following π-OBDD.

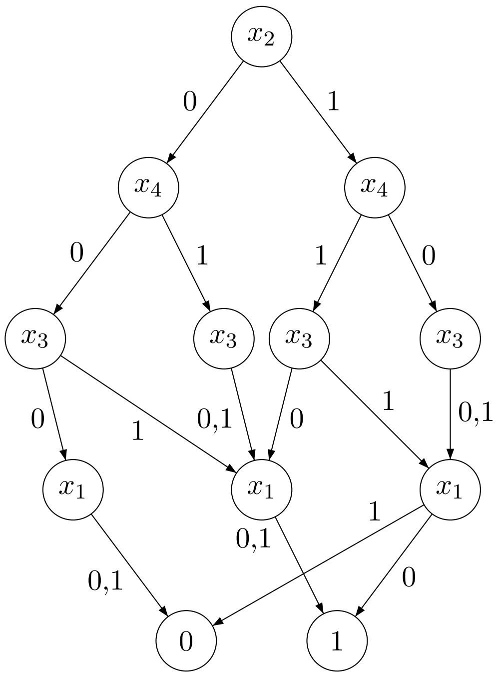

Figure 1: An OBDD with the permuation $\pi(1) = 2$, $\pi(2) = 4$, $\pi(3) = 3$, $\pi(4) = 1$

Given a permutation π over $\{1, \ldots, n\}$ and a Boolean function $f : \{0,1\}^n \to \{0,1\}$, it is possible to assign it a π-OBDD with a minimal number of nodes which is unique up to isomorphism, known as its *quasi-reduced* π-OBDD, whose *size* (i.e., its number of nodes) is denoted by π-OBDD(f). It is equivalent to saying that two nodes u and v labeled by the same variable whose 0-outgoing and 1-outgoing edges lead to the same node are equal. The notion of reduced OBDD introduced in [1] requires furthermore that the edges of a given node lead to different nodes, but we shall not use it. Indeed, the size of the quasi-reduced OBDD is within a factor n of the size of the reduced one, which is negligible in view of the growth of the OBDD as a function of n, see Theorems 2.

Consider two paths in a decision diagram, labeled by the same variable. The two nodes reached by these two paths are sources of two subdiagrams defining partial Boolean functions. If these functions are different then so are the two nodes in the quasi-reduced OBDD. But actually the following technical result tells more. It says that under certain hypotheses these two nodes may be proved different even when some of the the remaining variables have fixed values. For example, consider the leftmost two nodes of figure 1 at level 3 which are both labeled by the variable x_3. They define Boolean functions of the variables x_3 and x_1. These two functions are seen to be different even with the constraint assigning the value 0 to the variable x_3. This is the main tool for proving lower bounds on the quasi-reduced OBDD computing a given Boolean function.

Proposition 1. *Let $f : \{0,1\}^n \to \{0,1\}$ be a Boolean function and let $\pi \in \mathfrak{S}_n$ be a permution. Consider an integer $m \leq n$, a subset $I \subseteq \{1, \cdots, n\}$ disjoint from $\pi(\{1, \cdots, m\})$ of cardinality k and for each $i \in I$, a value $c_i \in \{0,1\}$. Let v be the assignment defined by $v(x_{\pi(i)}) = a_i$, $1 \leq i \leq m$ and $v(x_j) = c_j$, $j \in I$. Assume the following functions*

$$f_{|v} : \{0,1\}^{n-m-k} \to \{0,1\}$$

are all different when the a_i's vary in the set $\{0,1\}$. Then the size of the quasi-reduced OBDD computing f is greater than or equal to 2^m.

Proof. The arguments are (very) reminiscent of those developed in the theory of finite automata. Indeed, it suffices to verify that there are at least 2^m different nodes at level m of the diagram (recall that these nodes are labeled by the variable $x_{\pi(m)}$). By the definition of a quasi-reduced OBDD, this is equivalent to saying that two such different nodes define partial Boolean functions of the remaining variables $x_{\pi(m+1)}, x_{\pi(m+2)}, \ldots, x_{\pi(n)}$ which are different. But if these two partial functions are different when assigned fixed values to a subset of the remaining variables, they are all the more so when all remaining variables are free to take on arbitrary values. □

2.2 Sensitivity to the variable ordering

For a given Boolean function, the size of its quasi-reduced OBDD depends on the chosen ordering of the variables. The sensitivity of a Boolean function is the response of the ratio between the size of the smallest and the size of the greatest quasi-reduced OBDD when the orderings run over all possible permutations. For a random function this ratio is very close to 1, [4]. Now, instead of a unique Boolean function, consider a sequence $(f_n)_{n\in\mathbb{N}}$ of Boolean functions depending on n variables, not necessarily defined for all integers n. What can be said about the asymptotic behavior of the size of the reduced OBDD's recognizing the functions f_n? We use Wegener's classification into 5 categories. One of them assumes two conditions: the first one says that there exist orderings for which the size of the quasi-reduced OBDD grows as slowly as some polynomial. The second one assumes that there exists a fraction of orderings π tending to 1 when n tends to infinity, for which the size of the π-reduced OBDD has exponential growth. A more formal definition is as follows.

Definition 1. *A function $f = (f_n)$ is* nice *if there exists an integer k such that for all integers n for which the function f_n is defined and all permutations π_n the size of the π_n-OBDD(f_n) is less than n^k.*

Definition 2. *A function $f = (f_n)$ is* almost ugly *if the following two conditions are satisfied*

i) *there exists an integer k such that for all integers n for which the function f_n is defined there exists a permutation π_n for which the size of π_n-OBDD(f_n) is less than n^k.*

ii) *there exist a real number $\alpha > 1$ and for each integer n there exists a subset $\mathfrak{P}_n$ of permutations over n such that $\frac{|\mathfrak{P}_n|}{|\mathfrak{S}_n|} \underset{n\to\infty}{\to} 1$ with the following property. For all integers n for which the function f_n is defined and for all $\pi_n \in \mathfrak{P}_n$ the size of π_n-OBDD(f_n) is greater than α^n.*

E.g., the most significant bit of the sum of two binary integers and the comparison of two binary integers are examples of almost ugly functions, [5, Chapter 5].

2.3 Languages as Boolean functions

The free monoid generated by the alphabet $\Sigma = \{0,1\}$ is denoted by $\{0,1\}^*$ and the set of strings of length n by $\{0,1\}^n$. Given an arbitrary subset $X \subseteq \{0,1\}^*$ and an integer n, if $X \cap \{0,1\}^n \neq \emptyset$, we define the function $f_n : \{0,1\}^n \to \{0,1\}$ by setting

$$f_n(a) = \begin{cases} 1 \text{ if } a \in X \cap \{0,1\}^n \\ 0 \text{ if } a \in \{0,1\}^n - X \end{cases} \tag{1}$$

otherwise the function is not defined. It is the *characteristic function* of X for the strings of length n and can be viewed as a Boolean function, once the string $a = a_1 \cdots a_n$ is identified with the n-tuple of Boolean values $(a_1, \ldots, a_n)$. From now on, we will not distinguish between binary words of length n and n-tuples of values of Boolean variables. In particular, the i-th position of a generic binary word $x_1 \ldots x_n$ of length n will be viewed as a Boolean variable. The functions that we will consider are associated with languages *recognized* in finite groups, i.e., languages $X \subseteq \{0,1\}^*$ for which there exist a finite group G, a subset $K \subseteq G$ and a morphism $\phi : \{0,1\}^* \to G$ such that $X = \phi^{-1}(K)$. Here we concentrate on the case where K is reduced to the unit e of the group which is a very mild restriction. In other words, the functions f_n are defined as follows for all $x_1 \cdots x_n \in \{0,1\}^n$

$$f_n(x_1 \cdots x_n) = 1 \Leftrightarrow \phi(x_1 \cdots x_n) = \phi(x_1)\phi(x_2) \cdots \phi(x_n) = e$$

The expression $\phi(x_i)$ must be interpreted as a variable taking on values in the subset $\{\phi(0), \phi(1)\}$. The minimal finite automaton recognizing X processes the input sequentially and has linear size in n. Consequently, the quasi-reduced OBDD for the identity ordering satisfies the first condition of Definition 2. It just happens that for languages recognized in a finite group, the second condition of Definition 2 is satisfied under certain conditions.

3 A problem concerning groups

As said above, we are interested in the following problem. Given a morphism of the free monoid $\{0,1\}^*$ into a finite group G with unit e and $X = \phi(e)^{-1}$, we investigate the asymptotic behavior of the size of the quasi-reduced OBDD's computing the characteristic function of the subsets $X_n = X \cap \{0,1\}^n$.

Our result relies on a statistical property on permutations and on an algebraic property of finite non-abelian groups, see paragraph 3.2. We start with an example.

3.1 An example

We state a general condition under which the language associated with group is nice. It applies to various groups, for example, to the dihedral groups presented by $\langle a, b; a^2 = b^{4m} = 1, ab = b^{2m+1}a \rangle$ with $m \geq 1$, to the symmetric group on 3 elements generated by the two permutations (12) and (13) and to the group presented by $\langle a, b; a^4 = b^4 = 1, ab = b^3 a \rangle$.

Proposition 2. *Let G a group generated by two elements of even order satisfying $ab^2 = b^2 a$ and $ba^2 = a^2 b$. Let $\phi : \{0,1\}^* \to G$ be the morphism defined by $\phi(0) = a$ and $\phi(1) = b$. The set of words which map to the identity is nice.*

Proof. We have $ba = b^{-1}(ab)b = a^{-1}(ab)a$, $ab = a^{-1}(ba)a = b^{-1}(ba)b$, $a^2 = a^{-1}a^2 a = b^{-1}a^2 b$ and $b^2 = a^{-1}b^2 a = b^{-1}b^2 b$ which shows that a and

b have the same action by conjuacy on the subgroup $H \subseteq G$ represented by the words of even length. We want to evaluate the number of different subfunctions at level k of the quasi-reduced OBBD as defined by the Proposition 1. We recall that such a function is defined by the subdiagram hanging from a node labeled by $x_{\pi(k)}$. By grouping consecutive Boolean variables we may write the function under the form

$$f(u_0 y_1, u_1 \cdots y_p u_p) = 1 \Leftrightarrow \phi(u_0)\phi(y_1)\phi(u_1) \cdots \phi(u_{p-1})\phi(y_p)\phi(u_p) = e$$

with $p \leq k$, where the u's are, possibly empty, maximal sequences of consecutive variables with assigned values and the y's are maximum non empty sequences of consecutive variables with unassigned values. E.g., consider a function of $x_1 \cdots x_6 \in \{0,1\}^6$ into $\{0,1\}$. Assume the ordering of the variable to satisfy $\pi(1) = 4, \pi(2) = 3, \pi(3) = 1$, the morphism ϕ to be $\phi(0) = a$ and $\phi(1) = b$ and the 3 first visited variables to take on the values 1, 1 and 0 respectively. Then we have the equivalence

$$f(0x_2 11 x_5 x_6) = 1 \Leftrightarrow a\phi(x_2)bb\phi(x_5 x_6) = e$$

Consider another function g of level k, which in particular implies that the decomposition into alternate assigned and unassigned variables is the same

$$g(v_0 y_1 v_1 \cdots y_p v_p) = 1 \Leftrightarrow \phi(v_0)\phi(y_1)\phi(v_1) \cdots \phi(v_{p-1})\phi(y_p)\phi(v_p) = e$$

We claim that the two Boolean functions f and g are equal under all possible assignments to the y's if and only they are equal under some assignment which implies that there are at most as many functions as elements in G. Indeed, assume for some assignment $c_i = \phi(y_i)$, $i = 1, \ldots, p$, we have

$$\phi(u_0)c_1\phi(u_1) \cdots \phi(u_{p-1})c_p\phi(u_p) = \phi(v_0)c_1\phi(v_1) \cdots \phi(v_{p-1})c_p\phi(v_p)$$

Consider a new assignment $d_i = \phi(y_i)$ which coincides with c except for some $1 \leq \ell \leq p$: $c_\ell \neq d_\ell$. It suffices to prove that the following holds

$$\phi(u_0)d_1\phi(u_1) \cdots \phi(u_{p-1})d_p\phi(u_p) = \phi(v_0)d_1\phi(v_1) \cdots \phi(v_{p-1})d_p\phi(v_p)$$

Write

$$\begin{array}{ll} \phi(u_0)c_1\phi(u_1) \cdots \phi(u_{\ell-1}) = z_1, & \phi(u_\ell)c_{\ell+1} \ldots c_p\phi(u_p) = z_2 \\ \phi(v_0)c_1\phi(v_1) \cdots \phi(v_{\ell-1}) = t_1, & \phi(v_\ell)c_{\ell+1} \ldots c_p\phi(v_p) = t_2 \end{array}$$

The hypothesis implies $z_1 c_\ell t_1 = z_2 c_\ell t_2$, i.e., $t_2^{-1} c_\ell^{-1} z_2^{-1} z_1 c_\ell t_1 = 1$. Since the length (counted in the number of occurrences of generators) of the subsequence $z_2^{-1} z_1$ is even, it takes on its value in H under the two assignments

c and d. Since c_ℓ and d_ℓ are the values of the same subsequence under two different assignments, by the preliminary remark on the actions of the generators by conjugacy, the two elements $c_\ell^{-1}z_2^{-1}z_1c_\ell$ and $d_\ell^{-1}z_2^{-1}z_1d_\ell$ are equal. As a consequence, the number of possible different subfunctions at level k is bounded by the cardinality of G and the OBDD has linear size whatever the permutation of the variables, which completes the proof.

□

3.2 A statistics on permutations

Given an integer n meant to tend to infinity, decompose the interval $[n] = \{1, \ldots, n\}$ into blocks of k consecutive elements, for a fixed integer k:

$$B_1 = \{1, \ldots, k\}, B_2 = \{k+1, \ldots, 2k\}, \ldots, B_{\lceil \frac{n}{k} \rceil} = \{k(\lceil \frac{n}{k} \rceil - 1) + 1, \ldots, n\}$$

From now on, the term block refers to any of these $\lfloor \frac{n}{k} \rfloor$ subsets. By abuse of language, the subset $\{1, \ldots, \lfloor \frac{n}{2} \rfloor\}$ (respectively $\{\lfloor \frac{n}{2} + 1 \rfloor, \ldots, n\}$) is called *first half interval* (respectively *second half interval*). Call *template* every subset of $\{1, \ldots, k\}$. Given a template T and a permutation $\pi \in \mathfrak{S}_n$, we say that T occurs in block B_i if the set of variables in B_i which are queried in the first half interval are those whose indices belong to the subset $ik + T = \{ik + \ell \mid \ell \in T\}$, i.e.,

$$B_i \cap \pi(\{1, \ldots, \lfloor \frac{n}{2} \rfloor\}) = k(i-1) + T$$

the subset $k(i-1) + T$ is the *occurrence* of T in block B_i. The following is a weakening of [2, theorem 1].

Theorem 1. *With the previous notations, for every given $\epsilon > 0$, the probability that the fraction of blocks having an occurrence of a given template for a random permutation in the uniform distribution belongs to the interval $[\frac{1}{2^k} - \epsilon, \frac{1}{2^k} + \epsilon]$, tends to 1 when n tends to infinity.*

3.3 The theorem

Let m be an integer, G a group and Z its center (i.e., the subgroup of all the elements x which commute with all $y \in G$) and set $|G/Z| = p$. To each m-tuple $\mathbf{a} = (a_1, a_2, \ldots, a_m) \in G^m$ associate the function

$$\phi_{\mathbf{a}}(x_0, x_1, x_2, \ldots, x_m) = x_0a_1x_1a_2x_2 \ldots a_mx_m \tag{2}$$

Lemma 1. *the number of different functions of the form (2) is equal to* $|Z| \times p^{m-1}$.

Proof. It suffices to show, by setting $\mathbf{b} = (b_1, b_2, \ldots, b_m)$, that for any two functions $\phi_{\mathbf{a}}$ and $\phi_{\mathbf{b}}$ we identically have

$$\phi_{\mathbf{a}}(x_1, x_2, \ldots, x_m) = \phi_{\mathbf{b}}(x_1, x_2, \ldots, x_m) \tag{3}$$

if and only if for $i = 1, \ldots, m$ the condition $a_i^{-1} b_i \in Z$ holds and so does equality $a_0^{-1} b_0 \cdots a_m^{-1} b_m = 1$.

Indeed, let successively $a_m b_m^{-1}$, $a_{m-1} b_{m-1}^{-1}$, $\ldots$, $a_1 b_1^{-1}$ migrate towards the right of the formula.

$$\begin{aligned}
&x_0 a_1 x_1 \cdots a_m x_m x_m^{-1} b_m^{-1} x_{m-1}^{-1} b_{m-1}^{-1} \cdots x_1^{-1} b_1^{-1} x_0^{-1} \\
&= x_0 a_1 x_1 \cdots a_{m-1} x_{m-1} x_{m-1}^{-1} b_{m-1}^{-1} x_{m-2}^{-1} b_{m-2}^{-1} \cdots\cdots x_1^{-1} b_1^{-1} x_0^{-1} a_m b_m^{-1} \\
&\cdots \\
&= a_1 b_1^{-1} \cdots a_m b_m^{-1}
\end{aligned}$$

Conversely, if equality 3 is satisfied, then we identically have

$$x_1 a_2 x_2 \cdots a_m x_m x_m^{-1} b_m^{-1} x_{m-1}^{-1} b_{m-1}^{-1} \cdots b_2^{-1} x_1^{-1} = a_1^{-1} b_1$$

which shows, by letting x_1 vary, that $a_1^{-1} b_1$ belongs to the center. In particular we identically have

$$a_2 x_2 \cdots a_m x_m x_m^{-1} b_m^{-1} x_{m-1}^{-1} b_{m-1}^{-1} \cdots b_2^{-1} = a_1^{-1} b_1$$

Repeating the same process

$$x_2 a_3 \cdots a_m x_m x_m^{-1} b_m^{-1} x_{m-1}^{-1} b_{m-1}^{-1} \cdots b_3^{-1} x_2^{-1} = a_2^{-1} b_2 a_1^{-1} b_1$$

which shows that $a_2^{-1} b_2 a_1^{-1} b_1$ and therefore $a_2^{-1} b_2$ belongs to the center. In the end we obtain

$$e = a_m^{-1} b_m \cdots a_1^{-1} b_1$$

where all $a_i^{-1} b_i$'s belong to the center.

□

Theorem 2. *Let G be a finite non commutative group, generated by a, b. Let $\phi : \{0,1\}^* \to G$ be a morphism and $X = \phi(e)^{-1}$ where e is the unit of G. Assume there exists an integer k such that $G = \phi(\{0,1\}^k)$. Then X is almost ugly.*

Observe that the Theorem applies whenever the orders r and s of the generators a and b are coprime. Indeed, let ℓ be the smallest integer such that each element of G is the image by ϕ of a word of length at most equal to ℓ. As r and s are coprime, every integer greater than rs can be written as $ar + bs$ where $a, b \in \mathbb{N}$. By posing $k = \ell + rs$ we have

$$G = \phi(\{0,1\}^k) = \phi(\{0,1\}^{k+1}) = \dots$$

Proof. Since the language X is recognizable by a finite automaton having, say p states, given a fixed integer n, the quasi-reduced π-OBDD where π the identity permutation computing the characteristic funcion of the subset $X \cap \{0,1\}^n$ has size bounded by np which proves that condition (i) of definition 2 is satisfied.

Let us now turn to condition (ii). We assume without loss of generality that k divides the order of $\phi(0)$: $\phi(0)^k = e$. Decompose the interval $\{1,\dots,n\}$ into blocks of size $2k$, $\{1,\dots,2k\}$, $\{2k+1,\dots,4k\}$, $\dots$, $\{2k(\lfloor \frac{n}{2k} \rfloor - 1),\dots,n\}$ and consider those, say $2pk+1, 2pk+2, \dots, 2pk+2k$ for which exactly the variables $x_{2pk+1}, x_{2pk+2}, \dots, x_{2pk+k}$ (i.e., the first half set of the variables) are visited after querying $\lfloor \frac{n}{2} \rfloor$ variables. Denote by $\mathcal{B}$ this set of blocks and enumerate them $B_0, B_1, B_2, \dots, B_m$ by increasing order of their first position and set

$$B_i = \{x_{2r_ik+1}, x_{2r_ik+2}, \dots, x_{2r_ik+2k}\}$$

where $0 \leq i \leq m$. Apply theorem 1 with the unique template $\{1,2,\dots,k\}$ in the set $\{1,2,\dots,2k\}$. The probability that the proportion of blocks in $\mathcal{B}$ is greater than $\frac{1}{2^{2k}} - \epsilon$ for any arbitrary $\epsilon > 0$ for a random permutation tends to 1 when n tends to infinity. Hence by choosing $\epsilon = \frac{1}{2^{2k+1}}$, the probability that m is greater than $\frac{n}{2k}\frac{1}{2^{2k+1}} = \frac{n}{k2^{2k+2}}$ tends to 1.

Now we define subfunctions by choosing values for the variables of the first half of each block B_i with $1 \leq i \leq m$. Furthermore, in order to distinguish the different subfunctions we only need a subset of the remaining variables to take on arbitrary values as discussed before Proposition 1. All variables not belonging to a block in $\mathcal{B}$ and all variables belonging to the k first variables in block B_0 are assigned the value 0. Now for each block B_i in $\mathcal{B}$, $1 \leq i \leq m$, arbitrarily choose a value for all variables $x_{2r_ik+1}, x_{2r_ik+2}, \dots, x_{2r_ik+k}$. Denote by v the valuation thus defined and set

$$a_i = \phi(v(x_{2r_ik+1}))\phi(v(x_{2r_ik+2}))\dots\phi(v(x_{2r_ik+k})) \in G \tag{4}$$

The resulting function depends on $(m+1)k$ variables

$$x_{2r_0k+k+1}, \dots x_{2r_0k+2k}, \dots x_{2r_mk+k}, \dots x_{2r_mk+2k}$$

Example. Set $n = 17$, $k = 4$ and let $B_1 = \{1, 2, 3, 4\}$, $B_2 = \{5, 6, 7, 8\}$ and $B_3 = \{13, 14, 15, 16\}$ be blocks in $\mathcal{B}$. Then the valuation v assigns the value 0 to the variables

$$x_1, x_2, x_9, x_{10}, x_{11}, x_{12}, x_{17}$$

Concerning the four variables x_5, x_6, x_{13}, x_{14} we might choose $v(x_5) = 1, v(x_6) = 0, v(x_{13}) = 1, v(x_{14}) = 1$ which would lead to the function

$$f(00x_3x_4\mathbf{10}x_7x_8 0000\mathbf{11}x_{15}x_{16}0)$$

where the four bold face constants could have been chosen arbitrarily. Among these subfunctions, we are interested in those for which the a_i are representatives of the cosets of the center of the group G. By setting $c = \phi(0^{n-2k\lfloor \frac{n}{2k} \rfloor})$ we obtain

$$f_{|v}(x_1 \cdots x_n) = 1 \Leftrightarrow \prod_{k<j\leq 2k} \phi(x_{2r_0k+j})(\prod_{1\leq i\leq m} a_i \prod_{k<j\leq 2k} \phi(x_{2r_ik+j}))c = e \tag{5}$$

where e is the identity of the group G. Let us make a change of variables

$$y_i = \begin{cases} \phi(x_{2r_ik+1}) \cdots \phi(x_{2r_ik+k}) \text{ if } 0 \leq i < m \\ \phi(x_{2r_ik+1}) \cdots \phi(x_{2r_ik+k})c \text{ if } i = m \end{cases}$$

Then the second expression of 5 can be written as

$$y_0a_1y_1a_2y_2 \ldots a_my_m = e \tag{6}$$

where, because of the hypothesis, the y's independently range over G. Let u and v be two distinct valuations of the variables y's. Then the two subfunctions $f_{|u}(x_1 \cdots x_n)$ and $f_{|v}(x_1 \cdots x_n)$ are equal if and only if the following holds for all $y_0, y_1 \cdots y_m \in G$

$$y_0a_1y_1a_2y_2 \ldots a_my_m = e \Leftrightarrow y_0b_1y_1b_2y_2 \ldots b_my_m = e$$

This last equivalence holds if and only if equality

$$y_0a_1y_1a_2y_2 \ldots a_my_m = y_0b_1y_1b_2y_2 \ldots b_my_m$$

holds for all $y_0, y_1 \cdots y_m \in G$. Lemma 1 shows that there exist $|Z|p^{m-1}$ subfunctions which completes the proof.

□

References

[1] R. Bryant. Graph-based algorithms for boolean function manipulation. *IEEE Transactions on Computers*, C-35(8):677–691, 1986.

[2] C. Choffrut and Y. Haddad. String matching with OBDD's. *Theoretical Computer Science*, 313:187–198, 2004.

[3] C. Y. Lee. Representation of switching circuits by binary-decision programs. *Bell System Technical Journal*, 38:985–999, 1959.

[4] I. Wegener. The size of reduced OBDDs and optimal read-once branching programs for almost all Boolean functions. *I.E.E.E. Trans. on Computers*, 43:1962–1969, 1994.

[5] I. Wegener. *Branching Programs and Binary Decision Diagrams – Theory and Applications*. SIAM Monographs on Discrete Methods and Applications, 2001.