Available online at www.sciencedirect.com
SCIENCE DIRECT®

European Journal of Combinatorics 26 (2005) 755–763

European Journal of Combinatorics

www.elsevier.com/locate/ejc

Note on the integer geometry of bitwise XOR

António Guedes de Oliveira[a,*], Diogo Oliveira e Silva[b]

[a] *Departamento de Matemática Pura, Centro de Matemática da Universidade do Porto, Universidade do Porto, Portugal*
[b] *Departamento de Matemática Pura, Universidade do Porto, Portugal*

Received 20 January 2004; accepted 23 March 2004
Available online 25 May 2004

Abstract

We consider the set $\mathbb{N}$ of non-negative integers together with a distance d defined as follows: given two integers $x, y \in \mathbb{N}$, $d(x, y)$ is, in binary notation, the result of performing, digit by digit, the "XOR" operation on (the binary notations of) x and y. Dawson, in Combinatorial Mathematics VIII, Geelong, 1980, Lecture Notes in Mathematics, 884 (1981) 136, considers this geometry and suggests the following construction: given k different integers $x_1, \ldots, x_k \in \mathbb{N}$, let V_i be the set of integers closer to x_i than to any x_j with $j \neq i$, for $i, j = 1, \ldots, k$. Let $\mathbb{V} = (V_1, \ldots, V_k)$ and $X = (x_1, \ldots, x_k)$. $\mathbb{V}$ is a partition of $\{0, 1, \ldots, 2^n - 1\}$ which, in general, does not determine X.

In this paper, we characterize the convex sets of this geometry: they are exactly the line segments. Given X and the partition $\mathbb{V}$ determined by X, we also characterize in easy terms the ordered sets $Y = (y_1, \ldots, y_k)$ that determine the same partition $\mathbb{V}$. This, in particular, extends one of the main results of Combinatorial Mathematics VIII, Geelong, 1980, Lecture Notes in Mathematics, 884 (1981) 136.

1. Introduction

Let us take two non-negative integers in binary form and consider the result of performing with them the typical computer "bitwise XOR operator". Dawson, in [1], regards this function, `(i, j)` $\mapsto$ `i^j` using the C language notation or $(x, y) \mapsto x \dot{\vee} y$ in the notation herein, *geometrically*, as a *distance* between the two integers.

* Corresponding address: Departamento de Matemática Pura, Faculdade de Ciências da U. Porto, Rua do Campo Alegre 687, P-4169-007 Porto, Portugal.
E-mail address: agoliv@fc.up.pt (A.G. de Oliveira).

0195-6698/$ - see front matter © 2004 Elsevier Ltd. All rights reserved.
doi:10.1016/j.ejc.2004.02.008

He considers also, given an ordered set $X = (x_1, x_2, \ldots, x_k)$ of such integers, the *Voronoy cells* determined by them, that is, the sets V_i of elements closer to x_i than to any x_j with $j \neq i$, for every $i, j = 1, 2, \ldots, k$. In particular, he proves that there exist sets $A_i \subseteq B_i$ such that an integer x belongs to V_i if and only if the set $\Omega(x)$ of the positions of the digits 1 (or *1-bits*) of x satisfies

$$A_i \subseteq \Omega(x) \subseteq B_i. \tag{1.1}$$

Set $X_i := \Omega(x_i)$ and let m_i and M_i be such that $\Omega(m_i) = A_i$ and $\Omega(M_i) = B_i$. Condition (1.1), in its turn, is true if and only if x contains 1-bits in all the positions where m_i contains 1-bits, and 0-bits in all the positions where M_i contains 0-bits. Hence, Dawson's statement can be rephrased, in computer slang, in a sentence like:

$$x \in V_i \Longleftrightarrow x \text{ matches, as a string, } \_\_01\_001\_11\_.$$

In [1], a certain *duality* is also considered: let $Y_i := X_i \,\Delta\, A_i \,\Delta\, B_i$, where by Δ we denote the symmetric difference of two sets, and let y_i be such that $Y_i = \Omega(y_i)$; then, in particular, $A_i = X_i \cap Y_i$ and $B_i = X_i \cup Y_i$. Let us call $X = (x_1, x_2, \ldots, x_k)$ *the initial k-tuple* and $Y = (y_1, y_2, \ldots, y_k)$ *the final k-tuple*. [1, Lemma 1.3] asserts that these rôles are interchangeable: if we use instead Y as the initial *k-tuple*, we end up with X as the final one, and the Voronoy cells are exactly the same.

In this paper, we proceed further into the study of this particular geometry:

First, we characterize the *line segments*, i.e., the sets of form

$$[x\ y] := \{z \in \mathbb{N}: d(x,z) + d(z,y) = d(x,y)\};$$

they are the *intervals*, as we call the sets of the solutions of a condition like (1.1) above.

We also prove that, given $x, y \in \mathbb{N}$, the set

$$S(x,y) := \{z \in \mathbb{N}: z \dot{\vee} x < z \dot{\vee} y\}$$

is *convex*, in the sense that if it contains both points a and b then it contains all the segment $[a\ b]$. And we prove that *any* convex set is in fact a line segment (and vice versa).

As the main result, we characterize, given $X = (x_1, \ldots, x_k)$, the ordered sets $Z = (z_1, \ldots, z_k)$ with the same partition as X. More precisely (cf. Corollary 2.16), let $\mathbb{V}(X) = (V_1, \ldots, V_k)$ ($\mathbb{V}(X)$ is then the *Voronoy diagram* determined by X); we prove that $\mathbb{V}(Z) = \mathbb{V}(X)$ if and only if:

$$\forall\, i = 1, 2, \ldots, k, \qquad \forall\, j = 1, 2, \ldots, k, \qquad j \neq i \Longrightarrow \begin{cases} z_i \dot{\vee} x_j > z_i \dot{\vee} x_i \\ z_j \dot{\vee} x_i > z_i \dot{\vee} x_i. \end{cases}$$

Dawson's duality, referred to above, can be obtained from here.

Finally, we also prove that taking $(m_1, m_2, \ldots, m_k)$ or $(M_1, M_2, \ldots, M_k)$ as the initial k-tuple leads to the same Voronoy diagrams, whence making it easy to reverse Dawson's construction.

2. Bitwise XOR geometry

2.1. Notation, examples and technical results

Definition 2.1. Let $\mathbb{N}$ be the set of non-negative integers, and fix an integer $n > 0$. Let $\mho$ be the bijective function defined, for $A \subseteq \{1, 2, \ldots, n\}$, by:

$$\mho(A) := \sum_{i \in A} 2^{i-1}$$

and let $\Omega = \mho^{-1}$.

Denote by $x \dot\vee y$ the integer for which the binary representation has the ith digit (from right to left) equal to 1 if the ith digits of x and y are different, and equal to 0 if they are equal, for $i = 1, 2, \ldots, n$. This is the result of the "bitwise XOR operator", which is used, for example, for finding a winning strategy of the "celebrated game of Nim" [2, p. 44]. More precisely:

Definition 2.2. Let $a = \sum_{i=0}^{n-1} \alpha_i 2^i$ and $b = \sum_{i=0}^{n-1} \beta_i 2^i$ be such that $\alpha_i, \beta_i \in \{0, 1\}$ for all $i = 0, \ldots, n-1$. Then,

$$a \dot\vee b := \sum_{i=0}^{n-1} (\alpha_i \dot\vee \beta_i) 2^i,$$

where $0 \dot\vee 0 = 1 \dot\vee 1 = 0$ and $0 \dot\vee 1 = 1 \dot\vee 0 = 1$. In other words, $a \dot\vee b = \mho(\Omega(a) \,\Delta\, \Omega(b))$.

Following Dawson, we fix a set $\{x_1, \ldots, x_k\} \subseteq \mathbb{N}$ of $k > 0$ distinct integers smaller than 2^n, and define α: $\{0, 1, \ldots, 2^n - 1\} \to \{x_1, \ldots, x_k\}$ so that $z \dot\vee \alpha(z)$, for each z, is as small as possible. Then, for every $i \in \{1, \ldots, k\}$,

$$V_i := \alpha^{-1}(x_i) = \{z \in \mathbb{N} : \forall j = 1, \ldots, k \ (j \neq i), z \dot\vee x_j > z \dot\vee x_i\}.$$

Note that $\mathbb{V} := \{V_1, \ldots, V_k\}$ is a partition of $\{0, \ldots, 2^n - 1\}$, i.e., the latter set is the union of the elements of $\mathbb{V}$, that are non-empty and pairwise disjoint (since $a \dot\vee x = a \dot\vee y \Longrightarrow x = y$). We call it the *partition determined by* $X = (x_1, \ldots, x_k)$; for emphasizing its origin, we also denote it by $\mathbb{V}(X)$ and V_i by $\mathbb{V}(X, i)$. Bitwise AND and OR are defined similarly to Definition 2.2, and will also be denoted simply by $\wedge$ and $\vee$.

Definition 2.3. Given non-negative integers $a, b \in \mathbb{N}$, we say a is strongly less than b, written $a \prec b$, if $a \wedge b = a$ and $a \vee b = b$.

$$\langle a, b \rangle := \{c \in \mathbb{N}\colon a \prec c \prec b\}$$

is also called an *interval*.

Note that

$$a \prec b \Longleftrightarrow \Omega(a) \subseteq \Omega(b) \ (\Longrightarrow a < b)$$

and that x satisfies condition (1.1) if and only if $x \in \langle \mho(A_i), \mho(B_i) \rangle$.

Example 2.4. Take $m_i = \mho(\{2,3,5,9\})$, $M_i = \mho(\{1,2,3,4,5,8,9,11,12\})$ $(n = 12)$ and $V_i = \langle m_i, M_i \rangle$.

$$\begin{array}{lllll} m_i &= 278 &= 00\ 01\ 0\ 001\ 0\ 11\ 0_{(2)} & \text{and} \\ M_i &= 3487 &= 11\ 01\ 1\ 001\ 1\ 11\ 1_{(2)}. \end{array}$$

The elements of V_i are exactly the integers whose binary representations match the pattern:

$$\_\_\ 01\ \_\ 001\ \_\ 11\ \_.$$

We note that $(\{0,1\}, \dot\vee)$ may be naturally identified with $\mathbb{Z}/2\mathbb{Z}$. In particular, for example, $(a \dot\vee b) \dot\vee c = a \dot\vee (b \dot\vee c)$, $a \dot\vee b = b \dot\vee a$, $0 \dot\vee a = a$ and $a \dot\vee a = 0$ for all $a, b, c \in \mathbb{N}$. Note also that $(a, b) \mapsto a \dot\vee b$ *defines indeed a distance in* $\mathbb{N}$. In fact,

$$\sum_{i=0}^{n-1} \alpha_i 2^i + \sum_{i=0}^{n-1} \beta_i 2^i = \sum_{\substack{(\alpha_i,\beta_i)\neq(1,1) \\ 0\le i\le n-1}} (\alpha_i + \beta_i) 2^i + \sum_{0\le i\le n-1} 2 \cdot 2^i,$$

and $\alpha_i + \beta_i = \alpha_i \dot\vee \beta_i$ and $\alpha_i \wedge \beta_i = 0$ except when $\alpha_i = \beta_i = 1$. Hence,

$$a + b = a \dot\vee b + 2(a \wedge b) \tag{2.2}$$

and so $a \dot\vee b = (a \dot\vee c) \dot\vee (c \dot\vee b) \le a \dot\vee c + c \dot\vee b$.

Lemma 2.5. *Let* $a, b, c \in \mathbb{N}$. *Then, the following conditions are equivalent:*

$$c \in [a\ b] \overset{\text{def}}{\Longleftrightarrow} a \dot\vee b = a \dot\vee c + c \dot\vee b \tag{2.3}$$

$$a \wedge b \prec c \prec a \vee b. \tag{2.4}$$

Proof. Set $a = \sum_{i=0}^{n-1} \alpha_i 2^i$, $b = \sum_{i=0}^{n-1} \beta_i 2^i$ and $c = \sum_{i=0}^{n-1} \gamma_i 2^i (\alpha_i, \beta_i, \gamma_i \in \{0,1\}$ for all $i = 0, 1, \ldots, n-1)$.

$$\begin{aligned} c \in [a\ b] &\Longleftrightarrow (a \dot\vee c) \dot\vee (c \dot\vee b) = (a \dot\vee c) + (c \dot\vee b) \\ &\overset{(2.2)}{\Longleftrightarrow} (a \dot\vee c) \wedge (c \dot\vee b) = 0 \\ &\Longleftrightarrow \forall i = 0, 1, \ldots, n-1, \alpha_i \dot\vee \gamma_i = 0 \text{ or } \gamma_i \dot\vee \beta_i = 0 \\ &\Longleftrightarrow \forall i = 0, 1, \ldots, n-1, \gamma_i = \alpha_i \text{ or } \gamma_i = \beta_i \\ &\Longleftrightarrow \forall i = 0, 1, \ldots, n-1, \alpha_i \wedge \beta_i \le \gamma_i \le \alpha_i \vee \beta_i \\ &\Longleftrightarrow a \wedge b \prec c \prec a \vee b. \quad \square \end{aligned} \tag{2.5}$$

Remark 2.6. By definition of line segment (and since e.g., $(c \dot\vee a) \dot\vee (c \dot\vee b) = a \dot\vee b$):

$$\{x \dot\vee c : c \in [a\ b]\} = [x \dot\vee a\ x \dot\vee b]. \tag{2.6}$$

2.2. The convex sets

Proposition 2.7. *Let* $x, y \in \mathbb{N}$, $x \neq y$, *and consider*

$$S(x, y) := \{z \in \mathbb{N} : z \dot\vee x < z \dot\vee y\}.$$

If $a, b \in S(x, y)$, then $[a\ b] \subseteq S(x, y)$, i.e., $S(x, y)$ is convex. V_i is convex too for every $i = 1, 2, \ldots, k$.

Proof. Let m be the biggest element of the set $\Omega(x \dot{\vee} y) = \Omega(x) \,\Delta\, \Omega(y)$. Since m is, by definition, the leftmost position of all bits where x and y differ, $x < y$ holds if and only if $m \notin \Omega(x)$ (or equivalently, if and only if $m \in \Omega(y)$). Now, since $\Omega(z \dot{\vee} x) \,\Delta\, \Omega(z \dot{\vee} y) = \Omega(x) \,\Delta\, \Omega(y)$,

$$z \in S(x, y) \qquad \text{if and only if } m \notin \Omega(z \dot{\vee} x). \tag{2.7}$$

Hence, if $a, b \in S(x, y)$ then $m \notin \Omega(a \dot{\vee} x)$, $\Omega(b \dot{\vee} x)$. In order to prove that also $m \notin \Omega(c \dot{\vee} x)$ for every $c \in [a\ b]$, it is sufficient to show that:

$$\begin{aligned} &\Omega(c \dot{\vee} x) \subseteq \Omega(a \dot{\vee} x)\Omega(b \dot{\vee} x) \\ &\quad \Longleftrightarrow c \dot{\vee} x \prec (a \dot{\vee} x) \vee (b \dot{\vee} x). \end{aligned} \tag{2.8}$$

But this condition holds, by (2.6). Finally, V_i is also convex because $V_i = \bigcap_{j \neq i} S(x_i, x_j)$. $\square$

V_i is in fact a line segment (cf. [1, Lemma 1.3]). More precisely, we have:

Proposition 2.8. *Let, for $i = 1, 2, \ldots, k$, $y_i \in \mathbb{N}$ be the element of V_i at greatest distance from x_i, i.e., such that, for all $0 \leq z < 2^n$, if $x_i \dot{\vee} z > x_i \dot{\vee} y_i$ then $z \notin V_i$. Then $V_i = [x_i\ y_i]$.*

Proof. $[x_i\ y_i] \subseteq V_i$ because the latter is convex. Assume, by contradiction, that there exists $z \in V_i \backslash [x_i\ y_i]$. By Lemma 2.5 (condition (2.5) fails), for some j with $1 \leq j \leq k$ the jth bit of z is different from the jth bit of both x_i and y_i (that are equal, consequently).

For clearness sake, set $x = x_i$, $y = y_i$ and $y' = y \dot{\vee} 2^{j-1}$. Then y''s sth bit is equal to y's sth bit for all $s \neq j$, and is equal to z's sth bit (and hence different from the sth bit of both x and y) for $s = j$. Again by condition (2.5) of Lemma 2.5, $y' \in [z\ y]$. But then $y' \in V_i$, by convexity, which, since $x \dot{\vee} y' > x \dot{\vee} y$, is in contradiction with the definition of y_i. $\square$

Let $\mathcal{K}$ be any convex set, $x \in \mathcal{K}$ and y be the element of $\mathcal{K}$ farthest from x, as before. With the same proof, we obtain that $\mathcal{K}$ is a line segment, exactly $[x\ y]$. The converse is also true, by Lemma 2.5. Hence, we have:

Theorem 2.9. *Let $\mathcal{K}$ be a subset of $\{0, 1, \ldots, 2^n - 1\}$. Then:*

$$\mathcal{K} \text{ is convex} \Longleftrightarrow \mathcal{K} \text{ is a line segment.} \quad \square$$

2.3. Explicit calculation of Voronoy diagrams

Let us proceed a little further in the direction of the last result. As usual, by $\lfloor a \rfloor$ for a real number a we mean the biggest integer not bigger than a.

Definition 2.10. Set, for $X = (x_1, x_2, \ldots, x_k)$ and $i, j = 1, 2, \ldots, k, i \neq j$,

$$m_{ij}^X := \lfloor \log_2(x_i \dot{\vee} x_j) \rfloor + 1 \ (= \max(\Omega(x_i) \,\Delta\, \Omega(x_j));$$

$$Sm_i^X := \{m_{ij}^X : j = 1, 2, \ldots, k,\ j \neq i\}$$

$$a_i^X := \mho(Sm_i^X); \qquad b_i^X := \mho(\{1,\ldots,k\}\backslash Sm_i^X);$$
$$y_i^X := x_i \dot\vee b_i^X; \qquad m_i^X := x_i \wedge a_i^X; \qquad M_i^X := x_i \vee b_i^X.$$

(We drop the symbol X whenever it is not necessary.)

Remark 2.11. Denote by $\bar z$ the bitwise complement of $z \in \mathbb{N}$, $\bar z := (2^n - 1) \dot\vee z$. Then $b_i^X = \overline{a_i^X}$, and $a_i^X = (x_i \vee \overline{x_i}) \wedge a_i^X = (x_i \wedge a_i^X) \vee (\overline{x_i} \wedge a_i^X) = m_i^X \vee \overline{M_i^X}$.

We have the following theorem:

Theorem 2.12 (cf. [1, Lemmas 1.3 and 1.4]). *For every $X = (x_1, x_2, \ldots, x_k)$ and every $i = 1, 2, \ldots, k$,*

$$V_i = \mathbb{V}(X, i) = [x_i\ y_i^X] = \langle m_i^X, M_i^X\rangle. \tag{2.9}$$

Proof. We have seen before (condition (2.7)) that the condition $z \in S(x_i, x_j)$ is equivalent to $m_{ij} \notin \Omega(x_i \dot\vee z)$, or, in other words, to $2^{m_{ij}-1} \wedge (x_i \dot\vee z) = 0$. Hence,

$$z \in V_i = \bigcap_{j \neq i} S(x_i, x_j) \Longleftrightarrow a_i \wedge (x_i \dot\vee z) = 0.$$

By Proposition 2.8, however, $V_i = [x_i\ y_i]$ where y_i is the element $z \in V_i$ for which the value of $x_i \dot\vee z$ is maximum. But the maximum value of w for which $a_i \wedge w = 0$ is clearly $b_i = a_i \dot\vee (2^n - 1)$, the complement of a_i. Thus, the maximum is attained for z such that $x_i \dot\vee z = b_i \Longleftrightarrow z = x_i \dot\vee b_i$. Hence, this is the value of y_i. It is now easy to see, bitwise, that $m_i = x_i \wedge (x_i \dot\vee b_i) = x_i \wedge a_i$ and that $M_i = x_i \vee (x_i \dot\vee b_i) = x_i \vee b_i$ (e.g., $x_i \wedge (x_i \dot\vee b_i)$ is 1 exactly when $x_i = 1$ and $b_i = 0$). □

Theorem 2.13. *Let $X = (x_1, x_2, \ldots, x_k)$ for a subset $\{x_1, x_2, \ldots, x_k\}$ of $\{0, 1, \ldots, 2^n - 1\}$ with k (distinct) elements and $X' = (x_1', x_2', \ldots, x_k')$ for another subset $\{x_1', x_2', \ldots, x_k'\}$ of the same set. Then $\mathbb{V}(X') = \mathbb{V}(X)$ if and only if, for every $i = 1, 2, \ldots, k$,*

$$x_i' \in \mathbb{V}(X, i); \tag{2.10}$$
$$Sm_i^X = Sm_i^{X'}. \tag{2.11}$$

Proof. Suppose first $\mathbb{V}(X') = \mathbb{V}(X)$. Then $x_i' \in \mathbb{V}(X', i) = \mathbb{V}(X, i)$ and, by Theorem 2.12, $m_i^X = m_i^{X'}$ and $M_i^X = M_i^{X'}$. Moreover, by Remark 2.11, $a_i^{X'} = m_i^{X'} \vee \overline{M_i^{X'}} = a_i^X$. This implies condition (2.11).

Conversely, suppose that $x_i \wedge a_i^X = m_i^X \prec x_i' \prec M_i^X = x_i \vee b_i^X$ and $a_i^X = a_i^{X'}$. Then $x_i \wedge a_i^X \prec x_i' \wedge a_i^X \prec (x_i \vee b_i^X) \wedge a_i^X$. But $(x_i \vee b_i^X) \wedge a_i^X = (x_i \wedge a_i^X) \vee (b_i^X \wedge a_i^X) = x_i \wedge a_i^X$, and so $m_i^{X'} = m_i^X$. The proof that $M_i^{X'} = M_i^X$ proceeds in a similar way. □

Corollary 2.14. *Let X be as in Theorem 2.13. Then the Voronoy diagram determined by X, $\mathbb{V}(X)$, equals the Voronoy diagram determined by any of the collections Y, A or B defined below:*

$$Y = (y_1^X, y_2^X, \ldots, y_k^X);$$
$$A = (m_1^X, m_2^X, \ldots, m_k^X);$$
$$B = (M_1^X, M_2^X, \ldots, M_k^X).$$

Proof. We prove that in all three cases $s := m_{ij}^X$ equals $m_{ij}^{X'}$ for all $i, j = 1, 2, \dots, k$ such that $i \neq j$. First, note that, for every $s' > s$, $s' \in Sm_i^X$ if and only if $s' \in Sm_j^X$ since the s'th bits of x_i and x_j are equal, and thus the s'th bits of a_i^X and a_j^X are also equal. Denote, for $x \in \mathbb{N}$ and s such that $1 \leq s \leq k$, the sth bit of x by ${}_sx$, and note that ${}_{s'}y_i = {}_{s'}y_j$ exactly when ${}_{s'}x_i = {}_{s'}x_j$, since $y_i = x_i \dot{\vee} b_i^X$ and $y_j = x_j \dot{\vee} b_j^X$. This proves that $m_{ij}^{X'} \leq s$ for $X' = (y_1^X, y_2^X, \dots, y_k^X)$. The same happens for the other definitions of X', by the same reasons.

Now, in order to show that also $m_{ij}^{X'} \geq s$, it is sufficient to prove that ${}_sy_i$ and ${}_sy_j$ (respectively, ${}_sm_i$ and ${}_sm_j$, and ${}_sM_i$ and ${}_sM_j$) are different. But by definition of $s = m_{ij}$, ${}_sx_i$ and ${}_sx_j$ are indeed different, and $s \in Sm_i \cap Sm_j$. It follows that ${}_sa_i = 1 = {}_sa_j$ and so ${}_sb_i = 0 = {}_sb_j$. Finally, ${}_sy_i = {}_sx_i \dot{\vee} 0 = {}_sx_i$, ${}_sm_i = {}_sx_i \wedge 1 = {}_sx_i$, ${}_sM_i = {}_sx_i \vee 0 = {}_sx_i$, and a similar situation occurs when we replace i by j. $\square$

Remark 2.15. By the definition of y_i^X, we obtain in the first case [1, Corollary 1.6]: when $X = (x_1, \dots, x_k)$ is replaced in Dawson's construction by $Y = (y_1, \dots, y_k)$, as defined above, we also find Y replaced by X. This is so because $b_i^X = b_i^Y$, by Theorem 2.13.

Corollary 2.16. *Let* $X = (x_1, x_2, \dots, x_k)$ *for a subset* $\{x_1, x_2, \dots, x_k\}$ *of* $\{0, 1, \dots, 2^n - 1\}$ *with* k *(distinct) elements and* $X' = (x_1', x_2', \dots, x_k')$ *for another subset* $\{x_1', x_2', \dots, x_k'\}$ *of the same set. Then* $\mathbb{V}(X') = \mathbb{V}(X)$ *if and only if, for every* $i = 1, 2, \dots, k$,

$$x_i' \in \mathbb{V}(X, i) \tag{2.10}$$

and

$$x_i \in \mathbb{V}(X', i) \tag{2.12}$$

or, equivalently, if and only if

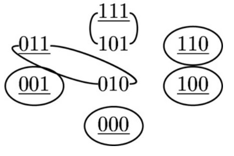
$$\forall i, j = 1, 2, \dots, k, \qquad j \neq i \Longrightarrow \begin{cases} x_i' \dot{\vee} x_j > x_i' \dot{\vee} x_i \\ x_j' \dot{\vee} x_i > x_i' \dot{\vee} x_i. \end{cases} \tag{2.13}$$

Proof. By symmetry, all we have to prove is that condition (2.12) (together with condition (2.10)) implies condition (2.11). Let us fix $i \in \{1, 2, \dots, n\}$ and set more simply $x := x_i$, $x' := x_i'$, $a := a_i^X$, $b := b_i^X$, $a' := a_i^{X'}$ and $b' := b_i^{X'}$. Since Condition (2.10) reads $x \wedge a \prec x' \prec x \vee b$, if, for $s = 1, 2, \dots, k$, we denote again by ${}_sa$ the sth bit of a and suppose ${}_sa = 1$ (and hence ${}_sb = 0$), then ${}_sx = {}_sx \wedge 1 \leq {}_sx' \leq {}_sx \vee 0 = {}_sx$, and so ${}_sx = {}_sx'$. In the same way, by condition (2.12), ${}_sa' = 1$ also implies ${}_sx = {}_sx'$. Coming back to our former notation, what we have shown is that x_i and x_i' coincide in all the 1-bits of a_i^X and in all the 1-bits of $a_i^{X'}$, which are the elements of Sm_i^X and $Sm_i^{X'}$, respectively.

Now suppose, for a contradiction, that condition (2.11) fails. Without loss of generality we may then suppose that there exist i, j $(i \neq j)$ such that $r := m_{ij}^X < s := m_{ij}^{X'}$. Then $s \in Sm_i^{X'} \cap Sm_j^{X'}$, and $s \notin \Omega(x_i \dot{\vee} x_j)$, but $s \in \Omega(x_i' \dot{\vee} x_j')$, which means that x_i and x_j have equal sth bits but the sth bits of x_i' and x_j' are different. But this is impossible since by our previous argument the sth bits of x_i and x_i' are equal, and the same happens with the sth bits of x_j and x_j'. $\square$

An interesting question arises as to whether all partitions of the set $\{0, 1, \ldots, 2^n - 1\}$ in k intervals can be constructed in this way from a set $\{x_1, x_2, \ldots, x_k\}$, when reorderings of $\{1, 2, \ldots, n\}$ are considered. We finish this section by showing through three small examples that the answer to this question is negative, and that conditions (2.10) and (2.11), separately, are not sufficient for forcing $\mathbb{V}(X) = \mathbb{V}(Y)$:

Example 2.17. Let $n = 3$ and consider the partition of $\{0 = 000_{(2)}, \ldots, 7 = 111_{(2)}\}$ represented below.

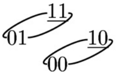


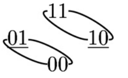
Suppose that the elements of form x_i are those we have underlined and, for a certain order $<_n$ of the elements of $\{1, 2, 3\}$, they determine the partition. We find a contradiction:

- $1 <_n 2$ since 010 is closer to 011 than to 000;
- $2 <_n 1$ since 101 is closer to 111 than to 100.

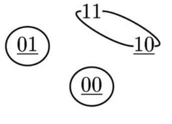
The other three possible choices of elements of $X = (x_1, \ldots, x_6)$ that could generate this partition can be discarded in a similar way.

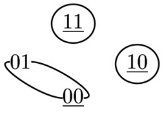
Example 2.18. Consider $X = (x_1, x_2) := (2 = 10_{(2)}, 3 = 11_{(2)})$ and $X' = (x'_1, x'_2) := (2 = 10_{(2)}, 1 = 01_{(2)})$ and the partitions they determine in $\{0, 1, 2, 3\}$. Then $x'_1 = x_1$ and $x'_2 \in \mathbb{V}(X, 2)$ but $\mathbb{V}(X) \neq \mathbb{V}(X')$.





Example 2.19. Finally, consider $X = (0 = 00_{(2)}, 1 = 01_{(2)}, 2 = 10_{(2)})$ and $X' = (2 = 10_{(2)}, 3 = 11_{(2)}, 0 = 00_{(2)})$ and the partitions they determine in $\{0, 1, 2, 3\}$. Although they have the same m_{ij} for every $i \neq j$ (in fact, as shown below, $x_i \dot{\vee} x_j = x'_i \dot{\vee} x'_j$), the partitions are different.





$\dot{\vee}$	00	01	10
00	00	01	10
01	01	00	11
10	10	11	00

$\dot{\vee}$	10	11	00
10	00	01	10
11	01	00	11
00	10	11	00

Acknowledgements

This research was partially supported by Fundação Calouste Gulbenkian through the Program “Novos Talentos em Matematica”. The first author’s research was partially supported by FCT and PRAXIS XXI through the Research Units Pluriannual Funding Program, and by the project POCTI/36563/MAT/2000.

References

[1] J.E. Dawson, A construction for a family of sets and its application to matroids, in: Combinatorial Mathematics VIII, Geelong, 1980, Lecture Notes in Mathematics, vol. 884, Springer, Berlin, New York, 1981, pp. 136–147.

[2] E.R. Berlekamp, J. Conway, R.K. Guy, Winning Ways for Your Mathematical Plays, Games in General, vol. 1, Academic Press, London, 1982.