Note on the integer geometry of bitwise XOR*

António Guedes de Oliveira†‡
Centro de Matemática da Universidade do Porto
Departamento de Matemática Pura
Universidade do Porto

Diogo Oliveira e Silva
Departamento de Matemática Pura
Universidade do Porto

Abstract

We consider the set $\mathbb{Z}_0^+$ of non-negative integers together with a distance d defined as follows: given two integers $x, y \in \mathbb{Z}_0^+$, $d(x, y)$ is, in binary notation, the result of performing, digit by digit, the "XOR" operation on (the binary notations of) x and y. Dawson, in [1], considers this geometry and suggests the following construction: given k different integers $x_1, \ldots, x_k \in \mathbb{Z}_0^+$, 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 $\mathcal{V} = (V_1, \ldots, V_k)$ and $X = (x_1, \ldots, x_k)$. $\mathcal{V}$ is a partition of $\{0, 2, \ldots, 2^n - 1\}$ 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 $\mathcal{V}$ determined by X, we also characterize in easy terms the ordered sets $Y = (y_1, \ldots, y_k)$ that determine the same partition $\mathcal{V}$. This, in particular, extends one of the main results of [1].

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, $(\mathtt{i}, \mathtt{j}) \mapsto \mathtt{i\hat{}j}$ as denoted in "C", *geometrically*, as a *distance* between the two integers.

*Research partially supported by Fundação Gulbenkian through the Program "Novos Talentos em Matemática"

†Corresponding author. Adress: 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

‡Research partially supported by FCT and PRAXIS XXI through the Research Units Pluriannual Funding Program, and by the project POCTI/36563/MAT/2000.

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 verifies

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

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 the 1-bits of x match those of m_i and the 0-bits match the 0-bits of M_i. Hence, Dawson's statement can be rephrased, in computer slang, in a sentence like:

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

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 *initial k-tuple* to $X = (x_1, x_2, \ldots, x_k)$ and *final k-tuple* to $Y = (y_1, y_2, \ldots, y_k)$. [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

$$[x\,y] := \left\{ z \in \mathbb{Z}_0^+ :\ d(x,z) + d(z,y) = d(x,y) \right\};$$

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

We also prove that, given $x, y \in \mathbb{Z}_0^+$, the set

$$S(x,y) := \left\{ z \in \mathbb{Z}_0^+ :\ z \,\dot\vee\, x < z \,\dot\vee\, y \right\}$$

is *convex*, in the sense that if it contains both points x and y then it contains all the segment $[x\,y]$. 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 4.7), let $\mathbb{P}(X) = (V_1, \ldots, V_k)$ ($\mathbb{P}(X)$ is then the *Voronoy diagram* determined by X); we prove that $\mathbb{P}(Z) = \mathbb{P}(X)$ if and only if:

$$\forall\, i = 1, 2, \ldots, k, \quad \forall j = 1, 2, \ldots, k, \quad j \neq i \implies z_i \,\dot\vee\, x_j, x_i \,\dot\vee\, z_j > z_i \,\dot\vee\, x_i.$$

Dawson's duality, referred 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.

1.1 Notation and examples

Definition 1.1. *Let $\mathbb{Z}_0^+$ 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 i.th digit (from right to left) equal to 1 if the i.th 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]. We note this game was proved to contain "implicitly the additive theory of all impartial games" (for playing on-line with a lesson on the strategy, see [4]). More precisely:

Definition 1.2. *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, $a \dot{\vee} b = \mho\left(\Omega(a) \, \Delta \, \Omega(b)\right)$.

It turns out that $(\mathbb{Z}_0^+, \dot{\vee})$ is indeed a metric space, with a number of surprising *geometric* properties. As an example, consider $3 = 11_{(2)} = 011_{(2)}$, $6 = 110_{(2)}$ and note that $101_{(2)} = 5$; hence, the distance between 3 and 6 is 5, $d(3, 6) = 5$. But also $d(3, 5) = 6$ and $d(5, 6) = 3$. The same happens in general. In particular, $d(a, \cdot) : \mathbb{Z}_0^+ \to \mathbb{Z}_0^+ : x \mapsto d(a, x)$ is a bijection (it is even auto-inverse, Cf. 2.3).

Following Dawson, we fix a set $\{x_1, \ldots, x_k\} \subseteq \mathbb{Z}_0^+$ of $k > 0$ distinct integers smaller than 2^n, and define $\alpha : \{0, 1, \ldots, 2^n - 1\} \to \{x_1, \ldots, x_k\}$ so that $z \dot{\vee} \alpha(z)$, for each z, is as small as possible. We look at the sets of form $V_i := \alpha^{-1}(x_i)$. Then

$$V_i = \left\{ z \in \mathbb{Z}_0^+ : \forall \, j = 1, \ldots, k \ (j \neq i), \quad z \dot{\vee} x_j > z \dot{\vee} x_i \right\}, \quad i = 1, \ldots, k.$$

Note that $\mathcal{V} = \{V_1, \ldots, V_k\} = \{\alpha^{-1}(x_1), \ldots, \alpha^{-1}(x_k)\}$ is a partition of $\{0, \ldots, 2^n - 1\}$, i.e., the latter set is the union of the elements of $\mathcal{V}$, that are non-empty and pairwise disjoint. We call it the *partition determined by* $X = (x_1, \ldots, x_k)$ and also denote the set V_i by $\mathbb{P}(X, i)$ and $(V_1, \ldots, V_k)$ by $\mathbb{P}(X)$ for emphasizing its origin.

Bitwise AND and OR are defined similarly to 1.2, and will also be denoted simply by $\wedge$ and $\vee$. We note they correspond to intersection and union of sets in the following sense: given $a, b \in \mathbb{Z}_0^+$, $a \wedge b = \mho\left(\Omega(a) \cap \Omega(b)\right)$ and $a \vee b = \mho\left(\Omega(a) \cup \Omega(b)\right)$.

Definition 1.3. *Given non-negative integers $a, b \in \mathbb{Z}_0^+$, we say a is* strongly less *than b, written $a \prec b$, if $a \wedge b = a$ and $a \vee b = b$.*

This is what we could call "bitwise less or equal to" since, clearly, $a \prec b$ if and only if, for every $i = 1, 2, \ldots, n$, the i.th bit of a is less or equal to the i.th bit of b. Hence,

$$a \prec b \iff \Omega(a) \subseteq \Omega(b)\big(\implies a < b\big).$$

We also call an *interval* a subset of $\mathbb{Z}_0^+$ of form:

$$\langle a, b\rangle := \big\{c \in \mathbb{Z}_0^+ :\ a \prec c \prec b\big\}.$$

Note that x verifies condition 1.1 if and only if $x \in \langle \mho(A_i), \mho(B_i)\rangle$. Let us consider an example:

Take $n = 12$, $A_i = \{2, 3, 5, 9\} = \Omega(m_i)$, $B_i = \{1, 2, 3, 4, 5, 8, 9, 11, 12\} = \Omega(M_i)$ and $V_i = \langle m_i, M_i\rangle$ Then,

$$\begin{array}{rcrcl} m_i & = & 278 & = & 00\ 01\ 0\ 001\ 0\ 11\ 0_{(2)}, \\ M_i & = & 3487 & = & 11\ 01\ 1\ 001\ 1\ 11\ 1_{(2)} \end{array}$$

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

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

2 Triangular (in)equality

We start this section by introducing some basic technical results.

Lemma 2.1. *Let $a, b, c \in \mathbb{Z}_0^+$ be any non-negative integers. Then*

$$(a \dot\vee b) \dot\vee c = a \dot\vee (b \dot\vee c),\ a \dot\vee b = b \dot\vee a, 0 \dot\vee a = a \text{ and } a \dot\vee a = 0; \tag{2.2}$$

$$b = a \dot\vee (a \dot\vee b); \tag{2.3}$$

$$a \dot\vee b \prec a \vee b, \text{ or, equivalently,}$$

$$(a \dot\vee b) \wedge (a \vee b) = a \dot\vee b \text{ and } (a \dot\vee b) \vee (a \vee b) = a \vee b; \tag{2.4}$$

$$(a \dot\vee b) \wedge (a \wedge b) = 0 \text{ and } (a \dot\vee b) \vee (a \wedge b) = a \vee b; \tag{2.5}$$

$$a + b = a \dot\vee b + 2(a \wedge b); \tag{2.6}$$

$$a \dot\vee b \leq (a \dot\vee c) + (c \dot\vee b); \tag{2.7}$$

Proof. Equations in 2.2 reflect the obvious fact that $(\mathbb{Z}_0^+, \dot\vee)$ may be naturally identified with $\mathbb{Z}/2\mathbb{Z}$, and 2.3 is a clear consequence of them. Equations in 2.4 and 2.5 have trivial bitwise verification.

In 2.6, it is used the fact that addition in binary or in any other base can be performed recursively in two steps: in a first one, the remainders are not considered; in a second one, the remainders are added up. Considered bitwise, in the first step it is performed the operation XOR; in the second (which gives either 0 or 1, and 1 exactly when both bits are equal to 1) it is AND that is performed, but the result is shifted leftwise. More precisely:

$$\begin{aligned}\sum_{i=0}^{n-1}\alpha_i\,2^i+\sum_{i=0}^{n-1}\beta_i\,2^i &= \sum_{\substack{(\alpha_i,\beta_i)\neq(1,1)\\ 0\le i\le n-1}}(\alpha_i+\beta_i)\,2^i+\sum_{\substack{\alpha_i=\beta_i=1\\ 0\le i\le n-1}}2\cdot 2^i\\ &= \sum_{i=0}^{n-1}(\alpha_i\,\dot\vee\,\beta_i)\,2^i+2\sum_{i=0}^{n-1}(\alpha_i\wedge\beta_i)\,2^i.\end{aligned}$$

Finally, for 2.7, we have $a\,\dot\vee\,b=(a\,\dot\vee\,c)\,\dot\vee\,(c\,\dot\vee\,b)$ (by 2.2) $\le a\,\dot\vee\,c+c\,\dot\vee\,b$ (by 2.6). □

Remark 2.2. By 2.2 and 2.7, $(a,b)\mapsto a\,\dot\vee\,b$ defines indeed a distance in $\mathbb{Z}_0^+$.

We remember the definition of *line segment*:

$$[x\,y]:=\left\{z\in\mathbb{Z}_0^+:\ x\,\dot\vee\,z+z\,\dot\vee\,y=x\,\dot\vee\,y\right\},\ \text{for } x,y\in\mathbb{Z}_0^+.$$

Proposition 2.3. *Set $a=\sum_{i=0}^{n-1}\alpha_i\,2^i$, $b=\sum_{i=0}^{n-1}\beta_i\,2^i$ and $c=\sum_{i=0}^{n-1}\gamma_i\,2^i$, with $\alpha_i,\beta_i,\gamma_i\in\{0,1\}$ for all $i=0,1,\dots,n-1$. The following conditions are equivalent:*

$$c\in[a\,b] \tag{2.8}$$

$$\forall\ i=0,1,\dots,n-1,\ \gamma_i=\alpha_i\ \text{or}\ \gamma_i=\beta_i; \tag{2.9}$$

$$a\wedge b\prec c\prec a\vee b \tag{2.10}$$

Proof.

$$\begin{aligned}2.8 &\overset{\text{def}}{\iff} a\,\dot\vee\,b=a\,\dot\vee\,c+c\,\dot\vee\,b\\ &\overset{2.2}{\iff}(a\,\dot\vee\,c)\,\dot\vee\,(c\,\dot\vee\,b)=(a\,\dot\vee\,c)+(c\,\dot\vee\,b)\\ &\overset{2.6}{\iff}(a\,\dot\vee\,c)\wedge(c\,\dot\vee\,b)=0\\ &\iff\forall\ i=0,1,\dots,n-1,\ \alpha_i\,\dot\vee\,\gamma_i=0\ \text{or}\ \gamma_i\,\dot\vee\,\beta_i=0\\ &\iff 2.9\\ &\iff\forall\ i=0,1,\dots,n-1,\ \alpha_i\wedge\beta_i\le\gamma_i\le\alpha_i\vee\beta_i\\ &\iff 2.10\end{aligned}$$

□

Remark 2.4. By definition of line segment (and since e.g. $(c \dot\vee a) \dot\vee (c \dot\vee b) = a \dot\vee b$):

$$\big\{x \dot\vee c : \ c \in [a\,b]\big\} \ = \ [x \dot\vee a \ x \dot\vee b]. \tag{2.11}$$

The ends of the interval $[x\,y] = \langle x \wedge y, x \vee y\rangle$ are not uniquely defined; in fact, if $b \in \langle a, c\rangle$ and $d = a \dot\vee b \dot\vee c$, then $[b\,d] = \langle a, c\rangle$.

(This can be seen with a Venn's diagram or with the following table, where α, β, γ and δ represent the possible values of a generic bit of a, b, c and d, respectively, with $\alpha \le \beta \le \gamma$:

α	β	γ	$\delta = \alpha \dot\vee \beta \dot\vee \gamma$	$\beta \wedge \delta$	$\beta \vee \delta$
0	0	0	0	0	0
0	0	1	1	0	1
0	1	1	0	0	1
1	1	1	1	1	1

)

3 The convex sets

Proposition 3.1. *Let $x, y \in \mathbb{Z}_0^+$, $x \neq y$, and consider*

$$S(x, y) := \big\{z \in \mathbb{Z}_0^+ : \ z \dot\vee x < z \dot\vee y\big\}.$$

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 $\Omega(z \dot\vee x) \ \Delta \ \Omega(z \dot\vee y) = \Omega(x) \ \Delta \ \Omega(y)$,

$$z \in S(x, y) \text{ if and only if } m \notin \Omega(z \dot\vee x). \tag{3.12}$$

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:

$$\begin{aligned} \mho(c \dot\vee x) \ &\subseteq \ \mho(a \dot\vee x) \cup (b \dot\vee x) \quad \Longleftrightarrow \\ c \dot\vee x \ &\prec \ (a \dot\vee x) \vee (b \dot\vee x). \end{aligned} \tag{3.13}$$

But this condition holds, by 2.11. Finally, V_i is also convex because $V_i = \cap_{j \neq i} S(x_i, x_j)$. □

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

Proposition 3.2. *Let, for $i = 1, 2, \ldots, k$, $y_i \in \mathbb{Z}_0^+$ be the element of V_i at greatest distance from x_i, i.e., such that, for all $0 \le z < 2^n$, 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 $z \in V_i \setminus [x_i\, y_i]$. By Proposition 2.3 (2.9 fails), for some j with $1 \leq j \leq k$ the j.th bit of z is different from the j.th 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 s.th bit is equal to y's s.th bit for all $s \neq j$, and is equal to z's s.th bit (and hence different from the s.th bit of both x and y) for $s = j$. Again by condition 2.9 of Proposition 2.3, $y' \in [z\, y]$. 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. □

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 $[x\, y]$ (Cf. Remark 2.4). The converse is also true, by Proposition 2.3. Hence, we have:

Theorem 3.3. *Let $\mathcal{K}$ be a subset of $\{0, 2, \ldots, 2^n - 1\}$. Then:*

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

4 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 4.1. *Set, for $X = (x_1, x_2, \ldots, x_k)$ and $i, j = 1, 2, \ldots, k$, $i \neq j$,*

$$\begin{gathered} m_{ij}^X := \lfloor \log_2(x_i \dot\vee x_j) \rfloor + 1 \quad (= \max(\Omega(x_i) \,\Delta\, \Omega(x_j))\,; \\ Sm_i^X := \left\{ m_{ij}^X :\ j = 1, 2, \ldots, k,\ j \neq i \right\} \\ a_i^X := \mho(Sm_i^X)\,; \quad b_i^X := \mho(\{1, \ldots, k\} \setminus Sm_i^X)\,; \\ y_i^X := x_i \dot\vee b_i^X; \quad m_i^X := x_i \wedge a_i^X; \quad M_i^X := x_i \vee b_i^X. \end{gathered}$$

(We drop the symbol X whenever not necessary.)

Remark 4.2. Denote by $\overline{z}$ the bitwise complement of $z \in \mathbb{Z}_0^+$, $\overline{z} := (2^n - 1) \dot\vee z$. 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 4.3. *For every $X = (x_1, x_2, \ldots, x_k)$ and every $i = 1, 2, \ldots, k$,*

$$V_i = \mathbb{P}(X, i) = [x_i\, y_i^X] = \langle m_i^X, M_i^X \rangle. \tag{4.14}$$

Proof. We have seen before (3.12) 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,

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

By Proposition 3.2, 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 $x_i \dot{\vee} z = b_i \iff z = x_i \dot{\vee} b_i$. Hence, this is 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 4.4. *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 $\mathbb{P}(X') = \mathbb{P}(X)$ if and only if, for every $i = 1, 2, \ldots, k$,*

$$x'_i \in \mathbb{P}(X, i); \tag{4.15}$$

$$Sm_i^X = Sm_i^{X'}. \tag{4.16}$$

Proof. Suppose first $\mathbb{P}(X') = \mathbb{P}(X)$. Then $x'_i \in \mathbb{P}(X', i) = \mathbb{P}(X, i)$ and, by Theorem 4.3, $m_i^X = m_i^{X'}$ and $M_i^X = M_i^{X'}$. Moreover, by Remark 4.2, $a_i^{X'} = m_i^{X'} \vee \overline{M_i^{X'}} = a_i^X$. This implies condition 4.16.

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 4.5. *Let X be as in Theorem 4.4. Then the Voronoy diagram determined by X, $\mathbb{P}(X)$, equals the Voronoy diagram determined by any of the collections Y, A or B defined below:*

$$\begin{aligned} Y &= (y_1^X, y_2^X, \ldots, y_k^X); \\ A &= (m_1^X, m_2^X, \ldots, m_k^X); \\ B &= (M_1^X, M_2^X, \ldots, M_k^X). \end{aligned}$$

Proof. We prove that in all three cases $s := m_{ij}^X$ equals $m_{ij}^{X'}$ for all $i, j = 1, 2, \ldots, k$ 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 $x \in \mathbb{Z}_0^+$ and s such that $1 \leq s \leq k$, the s.th 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 $X' = (y_1^X, y_2^X, \ldots, y_k^X)$. 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, ${}_sy_i = {}_sx_i \dot\vee 0 = 1 - {}_sx_i$, ${}_sm_i = {}_sx_i \wedge 1 = {}_sx_i$, ${}_sM_i = {}_sx_i \vee 0 = {}_sx_i$, and a similar situation occurs when we replace i by j. □

Remark 4.6. By the definition of y_i^X, we obtain in the first case [1, Corollary 1.6]: when $X = (x_1, \ldots, x_k)$ is replaced in Dawson's construction by $Y = (y_1, \ldots, y_k)$, as defined above, we also find Y replaced by X. This is so because $b_i^X = b_i^Y$, by Theorem 4.4.

Corollary 4.7. *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 $\mathbb{P}(X') = \mathbb{P}(X)$ if and only if, for every $i = 1, 2, \ldots, k$,*

$$x'_i \in \mathbb{P}(X, i) \tag{4.15}$$

and

$$x_i \in \mathbb{P}(X', i) \tag{4.17}$$

or, equivalently, if and only if

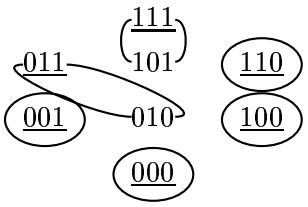
$$\forall\, i, j = 1, 2, \ldots, k, \quad j \neq i \implies x'_i \dot\vee x_j, x_i \dot\vee x'_j > x'_i \dot\vee x_i. \tag{4.18}$$

Proof. By symmetry, all we have to prove is that condition 4.17 (together with condition 4.15) implies condition 4.16. Let us fix $i = 1, 2, \ldots, n$ 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 4.15 reads $x \wedge a \prec x' \prec x \vee b$, if, for $s = 1, 2, \ldots, k$, we denote again by ${}_sa$ the s.th 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 4.17, ${}_sa' = 1$ 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 4.16 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 s.th bits but the s.th bits of x'_i and x'_j are different. But this is impossible since by our previous argument the s.th bits of x_i and x'_i are equal, and the same happens with the s.th bits of x_j and x'_j. □

An interesting question arises as to whether all partitions of the set $\{0, 1, \ldots, 2^n - 1\}$ in k intervals can be constructed this way 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 4.15 and 4.16, separately, are not sufficient for forcing $\mathbb{P}(X) = \mathbb{P}(Y)$:

Example 4.8. Consider the partition of $\{0=000_{(2)},\ldots,7=111_{(2)}\}$ represented below.

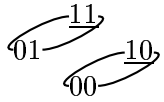


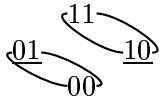
Suppose that the elements of form x_i are those that we have underlined and, for a certain order, they determine the partition. Then, we find a contradiction:

- $1 < 2$ since $2 = 010_{(2)}$ is closer to $3 = 011_{(2)}$ than to $0 = 000_{(2)}$;
- $2 < 1$ since $5 = 101_{(2)}$ is closer to $7 = 111_{(2)}$ than to $4 = 100_{(2)}$;

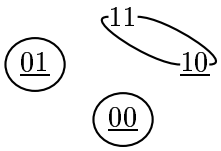
The other three possible choices of elements of $X = (x_1,\ldots,x_6)$ that could generate this partition can be discarded in a similar way.

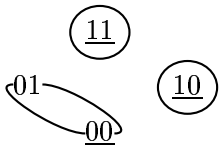
Example 4.9. Consider $X = (x_1,x_2) := (2 = 10_{(2)}\,,\, 3 = 11_{(2)})$ and $X' = (x'_1,x'_2) := (2 = 10_{(2)}\,,\, 1 = 01_{(2)})$ and the partitions they determine in $\{0,1,2,3\}$. Then $x'_1 = x_1$ and $x'_2 \in \mathbb{P}(X,2)$ but $\mathbb{P}(X) \neq \mathbb{P}(X')$.





Example 4.10. 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

References

[1] J.E. Dawson, "A construction for a family of sets and its application to matroids", *Combinatorial Mathematics VIII (Greelong, 1980)*, Lecture Notes in Math. **884**, Springer, Berlin-New York, 1981, pp. 136–147.

[2] Berlekamp, E.R.; Conway, J.; Guy, R.K., *Winning ways for your mathematical plays*, Vol. 1: Games in general. Academic Press, London (1982).

[3] Stahl, S., *A gentle introduction to game theory*, Amer. Math. Society, Providence (1999).

[4] `http://www.csm.astate.edu/Nim.html`