ON SET COUNTING AND ORDERING

Alina PETRESCU-NIȚĂ[1]

This paper presents some of properties of lattices and gives several examples of complete ordered monoids. Properties of the ordered sets relative to counting and searching are presented in section 2, and some counting consequences of countable sets are presented in section 3, the main results of the paper are proposition 3.1 and proposition 3.2.

Keywords: complet ordered monoid, ordered set, fixed point, countable set
2010 Mathematics Subject Classification: 06F05, 47H10, 03B25

1. Complete lattices, complete ordered monoids

Let M be a nonempty set and $\Delta_M = \{(x,x)/x \in M\}$ be the diagonal of M. If R is a binary relation on M, then by R^{-1} we denote the inverse relation and $RoR = \{(a,b) \in M \times M/\exists c \in M, aRc \text{ and } cRb\}$. Obviously, R is a partial order relation if and only if $\Delta_M \subset R, RoR \subset R,$ and $R \cap R^{-1} \subset \Delta_M$. We get a total order if $R \cup R^{-1} = M \times M$. Every pair ($M$, R), where R is a partial order relation, is called an ordered set or "poset". In this case, for a subset $A \subset M$ it is known the meaning of a majorant, max A, sup A, a maximal element and the duals of these.

Examples

1) If E is a nonempty set and $M = \mathcal{P}(E)$, ordered by inclusion, then for any $A, B \in M$, $\sup\{A, B\} = A \cup B$ and $\inf\{A, B\} = A \cap B$. Similarly, if V is a (real) vector space and M is the collection of the subspaces of V then for any $A, B \in M$, $\sup\{A, B\} = A + B$ and $\inf\{A, B\} = A \cap B$.

2) If $M = \mathbb{N}^*$ ordered by the relation of division "ı", then for any $a, b \in M$, $\sup\{a, b\} = cmmmc(a, b)$ and $\inf\{a, b\} = cmmdc(a, b)$.

Proposition 1.1. If N is a countable set and $M = \mathcal{P}(N)$, ordered by the inclusion, then the set M contains a totally ordered and non-countable subset.

Proof. We fix a bijective application $\varphi : N \to \mathbb{Q}$. For any real number α, we consider the set $X_\alpha = \{n \in N/\varphi(n) > \alpha\}$. The non-countable family (X_α), $\alpha \in \mathbb{R}$ is a totally ordered subset of M ; indeed, if $\alpha \leq \beta$, then $X_\beta \subset X_\alpha$.

[1] Lecturer, Mathematics Departament, University POLITHNICA of Bucharest, Romania, email: nita_alina@yahoo.com

Recall that a lattice is an ordered set $(L, \leq)$ such that for any $a, b \in L$, there exist $a \wedge b = \inf\{a, b\}$ and $a \vee b = \sup\{a, b\}$. The lattice is called complete if for any nonempty subset $S \subset L$, there exist sup S and inf S; [3], [5].

Example. $(\mathcal{P}(\mathrm{E}), \subseteq)$ is a complete lattice. The same occur for the lattice of subspaces of a vector space. Also, the collection of convex sets in $\mathbb{R}^n$ is complete, as well as $(\mathbb{N}^*, |)$. But $(\mathbb{Z}, \leq)$ is not a complete lattice, as well as the lattice $\mathbb{R}^n$ with the lexicographic order.

Proposition 1.2. A lattice $(L, \leq)$ is complete iff there exists max L and for any nonempty subset $S \subset L$, there exists inf S.

Proof. The implication direct is obvious since max L = sup L. For the converse implication, let $S \subset L$ and T be the set of majorants of S. Then T is nonempty (since max $L \in T$) and according to the assumption, there exists inf T. But this is sup S.

Corollary. Let M be a nonempty set and L be the equivalence relations set on M. Then L is a complete lattice relative to the inclusion.

Proof. Obviously, $M \times M = \max L$. According to the Proposition 1.2., it is sufficient to show that any collection $S = (R_i), i \in I$ of equivalence relations on M has an inferior margin, namely $\bigcap_{i \in I} R_i$ and this is in fact inf S.

Any monoid $(M, \cdot, e)$ is said to be a complete ordered monoid if it has and a structure of a complete lattice $(M, \leq)$ and moreover, for any subsets A, B of M, $\sup(A \cdot B) = (\sup A) \cdot (\sup B)$, where we denote $A \cdot B = \{a \cdot b / a \in A, b \in B\}$; [6].

If $(M', *, e')$ is another complete ordered monoid, then any morfism of monoids $f : M \to M'$ such that for any $A \subset M$, $f(\sup A) = \sup f(A)$ is calles morfism. In particular, if $x \leq y$ in M and we take $A = \{x, y\}$, then it follows that $f(x) \leq f(y)$ and, that means that the application f is monotone.

Proposition 1.3. If $(M, \cdot, e)$ is a monoid, then $(\mathcal{P}(E), \cdot, \{e\})$ is a complete ordered monoid.

Indeed, it is sufficient to show that for every two collection A, B of subsets of M, we have $\sup(A \cdot B) = (\sup A) \cdot (\sup B)$,

$$\text{i.e. } \bigcup_{c \in A \cdot B} c = \left(\bigcup_{a \in A} a\right) \cdot \left(\bigcup_{b \in B} b\right).$$

Corollary. If X is an arbitrary nonempty alphabet and $M = X^*$ is a free generated monoid by X (relative to the concatenation of words), then the set of languages relative to the product of the languages is a complete ordered monoid.

Proposition 1.4. If *M* is a nonempty set, then the set of equivalence relation on *M* is a complete ordered monoid relative to the composition of the relations, having Δ_M as neutral element.

Proof. According to Proposition 1.2., we have a complete lattice. It remains to show that the composition of the relations is distributive with respect to the unions, that is, for any collection *A, B* of equivalence relations on *M,* we have

$$\bigcup_{a\in A, b\in B}(a\cdot b)=\left(\bigcup_{a\in A}a\right)\cdot\left(\bigcup_{b\in B}b\right),$$

which is easy to verify.

In that follows, we give a special example of a complete ordered monoid.

Definition. We name calculation generator a 6-tuple $G=(S,I,T,\mathcal{P},\mathcal{R},\tau)$, where *S* is a finite set of states (or data sets), $I\subset S$ is the set of initial states, $T\subset S$ the set of terminal states, $\mathcal{P}$ is a collection of predicates on *S* (called conditions), $\mathcal{R}$ a collection of binary relations on *S* (called state transitions) and τ is an application $\tau:\mathcal{P}\to\mathcal{R}$ that associates to every predicate $p\in\mathcal{P}$ a transition $\tau(p)$; [7].

Since *S* is a finite set, it follows that the sets $I,T,\mathcal{P},\mathcal{R}$ are finite. Any condition $p\in\mathcal{P}$, is an application $p:S\to\mathbb{B},\mathbb{B}=\{0,1\}$, and any transition $\rho\in\mathcal{R}$ is a subset $\rho\subset S\times S$.

Let $s_0\in I$ be an initial state. Two cases appear:

a) If for any $p\in\mathcal{P}$ we have $p\ (s_0)=0$, then we consider that $s_0\in T$ and the generator stops.

b) If there exits $p\in\mathcal{P}$ such that $p(s_0)=1$, than we apply τ and let $\rho=\tau(p)$ be the associated transition. If there doesn't exist $s\in S$ such that $s_0\rho s$, then we consider $s\in T$ and the generator stops. On the contrary, there exists $s_1\in S$ such that $s_0\rho s_1$ and the previous generator process is restarted for s_1 in the same way it was applied for s_0 .

In this way we obtain a sequence of states $s_0,s_1,s_2,\ldots$ which is called calculation generated by *G*, starting with the state s_0. To every calculation generator *G* one may associate a graph having *S* as vertex set. The (finite) calculations appear as paths in this graph.

Proposition 1.5. If *G* is a calculation generator, than the set of the (finite) calculations sets is a completely ordered monoid.

Proof. Let $c=\{s_0,s_1,\ldots,s_m\}$ and $c'=\{t_1,t_2,\ldots,t_n\}$ be two calculation sets generated by *G.* These calculations are called compostable if $s_m=t_0$ and in this case, one define the calculation $c*c'=\{s_0,s_1,\ldots,s_m,t_1,\ldots,t_n\}$ of length

$m + n$ - 1. The operation "*" is not a concatenation. We consider the category G having just one subject, namely S, the morphisms being the calculations in S and the composition of morphisms is given by "*". If A, B are subsets of the set of morphisms, one define $A \cdot B = \{fg \,/\, f \in A,\ g \in B \text{ and } f, g \text{ compostable}\}$.

2. Ordered sets with the property PF.

The Knaster-Tarski fix point theorem is well known:" If $(L, \leq)$ is a complete lattice, then any monotone application $\varphi: L \to L$ has a fix point and the set of fixed points is a complete lattice relative to the relation " $\leq$ "; [2], [4], [5].

Let $(M, \leq)$ be an ordered set and $\varphi: M \to M$ be a monotone application; we denote $F_\varphi = \{x \in M \,/\, \varphi(x) = x\}$ the set of fix points of. We say that the set M has the property **PF** if for any monotone application $\varphi: M \to M$, the set F_φ is not empty.

The previous proposition shows that every complete lattice has the property **PF**.

If $(M, \leq)$ is a finite ordered set, one may consider the simplex complex $K(M)$ having the vertices the elements of M and as simplexes the chains of M (for example, $\{x_1 < x_2 < \cdots < x_n\} \subset M$ is a typical simplex).We denote by $|K(M)|$ the polyhedron defined by the simplex complex $K(M)$ with $H_q(M, \mathbb{Q})$ the group of rational homology in dimension q of $|K(M)|$; hence$H_q(M, \mathbb{Q}) = H_q(|K(M)|, \mathbb{Q})$. The ordered set M is called acyclic if $H_q(M, \mathbb{Q}) = 0$ for any $q \in \mathbb{Z}$. If M has just one element or if there exists $x \in M$ comparable with any other element of M, then M is acyclic. Baclawski ad Björner have proved in [1] that any finite ordered subset M and acyclic has the property **PF**.

We limit our interest to the study the ordering of finite sets by simple tools.

Let $(M, \leq)$ be a finite ordered set.

Proposition 2.1. For any two elements $a, b \in M$ with $a < b$, there exists a sequence $x_0 = a < x_1 < \cdots < x_k = b$ such that for any i, $1 \leq i \leq k$, we have $x_{i-1} \leq x_i$, if there doesn't exist $y \in M$ with $x_{i-1} < y < x_i$.

Proof. Let n be the number of those $y \in M$ for which $a < y < b$. We proceed by induction over n. For $n = 0$, the assertion is obvious, let us suppose $n \geq 1$ and let $a < c < b$. Then the number of those y for which $a < y < c$ and those z such that $c < z < b$ is at most $n-1$ (since we exclude c). According to the induction assumption, there exist sequences which connect a with c and c with b, and so these can be concatenate.

Proposition 2.2. The elements of M can be disposed such that

$M = \{x_1, x_2, \dots, x_n\}$ and $x_i < x_j$ if and only if $i < j$. (In this case we say that there exists a counting of the elements of *M* compatible with the order.)

Proof. Let $M = \{a_0, a_1, \dots, a_{n-1}\}$ and we denote $M_k = \{a_0, a_1, \dots, a_{k-1}\}$, for $1 \leq k \leq n$. Let $S_n = \{0, 1, \dots, n-1\}$ for any $n \geq 1$. We construct by induction the bijective application $\varphi_k: S_k \to S_k$, $1 \leq k \leq n$ such that if we denote $a_i^k = a_{\varphi_k(i)}, i \in S_k$, we have: $M_k = \{a_0^k, a_1^k, \dots, a_{k-1}^k\}$ and $a_i^k < a_j^k$ imply $i < j$. Then it follows that $M_n = M$ and we put $x_i = a_i^n$. For $k = 1$, φ_1 is unique determinate. We suppose that the bijective application $\varphi_{k-1}: S_{k-1} \to S_{k-1}$ is already constructed with the indicated property and let $p = \min\{i \in S_{k-1} / a_k < a_i^{k-1}\}$. We consider then the bijective application $\varphi_k: S_k \to S_k$ defined by $\varphi_k(i) = i$ if $i < p$; $\varphi_k(i) = k - 1$ if $i = p$ and $\varphi_k(i) = i - 1$ if $i > p$.

Remark. It is known that the winning numbers of a lottery are increasing ordered; similarly, looking for a word in a dictionary is simplified if these are ordered (for example, lexicographical).

If there exists an ordering like in Proposition 2.2, then to include a new element *u* between the elements of *M*, we have a problem of searching and we have *n* + 1 possibilities. If $x_k < u$ (for $1 \leq k \leq n$), it is established if the place is between 1 and *k* or between *k* + 1 and *n* + 1. If *k* is in the middle comparison $x_k < u$ is reduced twice. This is the halving algorithm. The number of comparisons is equal to $[\log_2(n+1)]$, where $[\alpha]$ is the smallest integer $\geq \alpha$.

As a consequence, any finite ordered set has minimal and maximal elements. We recover the following characterization of the finite sets (owned to Tarski):

Proposition 2.3. A set *M* is finite if and only if any nonempty subset of $\mathcal{P}(M)$ has a maximal element relative to the inclusion.

Proof. If *M* is finite, then $\mathcal{P}(M)$ is finite and has a maximal element. Conversely, if *M* would be infinite, then the set of finite parts of *M* would be a nonempty part of $\mathcal{P}(M)$, which has no maximal element.

Remark. Let $M = \{a_1, a_2, \dots, a_n\}$ be a finite set, with a given order of the elements. For any subset $T \subset M$, one can consider the sequence of *n* bits $c_1, c_2, \dots, c_n$, , where $c_k = 1$ if $a_k \in T$ and $c_k = 0$ on the contrary (for $1 \leq k \leq n$). Then the application $\varphi: \mathcal{P}(M) \to \mathbb{B}^n, T \to c_1 \dots c_n$ is bijective.

3. Counting

If *S* is a nonempty finite or countable set, every surjective application $v: \mathbb{N} \to S$ is called a counting of *S*.

Proposition 3.1. Any infinite subset $A \subset \mathbb{N}$ admits a counting $v: \mathbb{N} \to A$ (which can be called canonical).

Proof. For any $n \in \mathbb{N}$, we consider the application $f_n: S_n \to A$, $f_n(0) = \inf A$ and $f_n(k) = \inf(A \setminus \{f_n(0), \dots, f_n(k-1)\})$ for $1 \leq k \leq n$. If $S_n \subset S_m$ then $f_m \mid S_n = f_n$ and we define $v: \mathbb{N} \to A$ by $v \mid S_n = f_n$, for any $n \in \mathbb{N}$.

Let $p_1 < p_2 < \cdots < p_n < \cdots$ be the infinite sequence of prime numbers. We define an injective application on the free monoid $\mathcal{M}$ generated by $\mathbb{N}$ (must not be confused with $\mathbb{N} \setminus \{0\}$), $g: \mathcal{M} \to \mathbb{N}, g(\Lambda) = 0$ and for any $x_1 x_2 \dots x_k \in \mathbb{N}^k$, $g(x_1 x_2 \dots x_k) = p_1^{x_1} \cdot p_2^{x_2} \cdot \dots \cdot p_k^{x_k}$. In this way, we get a bijection $h: \mathcal{M} \to g(\mathcal{M})$ and $f = h^{-1} \circ v : \mathbb{N} \to g(\mathcal{M}) \to \mathcal{M}$ is a counting of $\mathcal{M}$.

Corollary. For any infinite alphabet *A* there exists a counting $v_A: \mathbb{N} \to A^*$.

It is sufficient to use the fact that the dictionary A^* is a countable set.

In 1873, G. Cantor proved that the set $\mathbb{R}$ is not countable and stated the conjecture that if $M \subset \mathbb{R}$ is a non-countable set, then it is equipotent with $\mathbb{R}$. In 1963, P. Cohen showed that this problem is non decidable in the usual system of axioms of Zermelo-Fraenkel (ZF) in the theory of sets. All mathematical theorems can be formulated according to these axioms. K. Gödel proved in 1931 that the axiomatique ZF (supposed to be non contradictory) is not complete, thas is, not any assertion formulated in this framework is decidable; [8].

The idea of the proof is based by the use of the prime numbers to obtain a adequate counting of the assertion in the system ZF, which isi in fact a formalization of the axiomatique $\mathcal{A}$ of arithmetic.

Any arithmetic formula is a syntactic word relative to the alphabet $\mathcal{A}$= {+, -, ×, …, 0, 1, …,9} and is a combination of different symbols to which we associate respectively code numbers; for example,

+ / **1**; - / **2**; × / **3**; : / **4**;) / **5**; (/ **6**; = / **7**; 0 / **8**; 1 / **9**; 2 / **10**; 3 / **11**; 4 / **12**; …; 9 / **17**.

We fix now the strict increasing sequence of the prime numbers: $p_1 = 2 < p_2 = 3 < p_3 = 5 < p_4 = 7 < \dots$; with the convention the arithmetic formula 1 + 2 = 3 has the Gödel code : $p_1^{\mathbf{9}} \cdot p_2^{\mathbf{1}} \cdot p_3^{\mathbf{10}} \cdot p_4^{\mathbf{7}} \cdot p_5^{\mathbf{11}} \equiv 2^{\mathbf{9}} \cdot 3^{\mathbf{1}} \cdot 5^{\mathbf{10}} \cdot 7^{\mathbf{7}} \cdot 11^{\mathbf{11}}$. Further, 1 $\equiv 2^{\mathbf{8}}$, and the number 120 = $2^{\mathbf{3}} \cdot 3^{\mathbf{1}} \cdot 5^{\mathbf{1}}$ decomposed in prime factors corresponds to the formula ×++ from A^*. The dot"•" is the symbol of multiplication and of concatenation. In this way, to any arithmetic formula (from A^*); one can associate just one natural number coded type Gödel and vice versa. We obtain now an injective application $A^* \to \mathbb{N}$. In the ZF axiomatic we further add a finite number of symbols (such as $\in$, $\cup$, $\cap$, { , } , as well as the variables *x, y, z,* etc.) and again the set of formulae is countable. Using a procedure that

reminds the diagonal of Cantor, Gödel had an assertion that is non decidable as well as his negation.

We illustrate this procedure as an answer to a simpler question.

In some papers of computer programming appear the assertion that any program $\mathcal{P}$, written in some programming language, associates to any initial data d a result $\mathcal{P}(d)$. To avoid the situation when the computer cycles (as in the case of writing the decimals for 2/3 or 1/7) or when the computer cannot finalize an operation, it would be useful to exist an algorithmic procedure that decide if the program $\mathcal{P}$ ends .

Proposition 3.2. These is no algorithmic procedure to decide if a program like $\mathcal{P}$ ends or not.

Proof. Let us suppose that there exists such procedure $\mathcal{A}$; the programs form a countable set and according to the Corollary of Proposition 3.1. these can be counted $p_0, p_1, \ldots, p_n, \ldots$. We suppose that for any input data d, the respective programs give the results $d_0, d_1, \ldots, d_n, \ldots$.
Then, we consider the following infinite matrix :

$$\begin{array}{llll} p_0(d_0) & p_0(d_1) & \ldots & p_0(d_n) \ \ldots \\ p_1(d_0) & p_1(d_1) & \ldots & p_1(d_n) \ \ldots \\ \ldots\ldots\ldots\ldots\ldots\ldots & & & \\ p_m(d_0) & p_m(d_1) & \ldots & p_m(d_n) \ \ldots \\ \ldots\ldots\ldots\ldots\ldots\ldots & & & \end{array}$$

and take the diagonal, that is the sequence of results $p_0(d_0), p_1(d_1), \ldots, p_k(d_k), \ldots$. Now, let us consider the program $\mathcal{P}$ which associates to any data $d \equiv d_n$, the result $\mathcal{P}(d) = p_d(d) + 1$ if the result $p_d(d)$ is attained, and $\mathcal{P}(d) = 0$ on the contrary. According to the assumption, this program is finalized by the procedure $\mathcal{A}$, so it coincides with one of the programs of the previous sequence; for example $\mathcal{P} = p_m$. Two situations erase: either $p_m(m)$ is not defined and then $\mathcal{P}(m) = 0$ (that is $\mathcal{P}(m) \neq p_m(m)$, contradiction), or $p_m(m)$ is defined and then $\mathcal{P}(m) = p_m(m) + 1$ (that is $\mathcal{P}(m) \neq p_m(m)$, again a contradiction).

REFERENCES

[1] *Baclawski, K., Björner A.*- Fixed Points in Partially Ordered Sets, Advances in math., 31, 263-287, 1979.

[2] *Blyth, T.S.* - Lattices and ordered Algebraic Structures, Springer, Berlin, 2005.

[3] *Căzănescu, V.,* Introducere în teoria limbajelor formale (Introduction to the Theory of formal languages), Ed. Academiei Române, 1983 (in Romanian)

[4] *Rus, I.*- Principii şi aplicaţii ale teoriei punctului fix (Principles and applications of fixed point theory), Ed. Dacia, Cluj-Napoca, 1979

[5] *Scott, D.*- Continous lattices, Lecture Notes in Math., 274, 1972

[6] *Stănăşilă, O*.- Notiuni şi tehnici de matematică discretă (Discrete mathematics concepts and techniques), Ed. Ştiinţifică şi Enciclop., Bucureşti, 1985 (in Romanian)
[7] *Thantcher, J.W., Wagner, E.G., Wright, J.B*.- Notes on algebraic fundamentals for theoretical computer Science, I.B.M. Thomas Watson, 109, 1979.
[8] *Țiplea, F*.- Fundamentele algebrice ale informaticii (The algebraic foundamentals of computer science), Editura Polirom, Bucureşti, 2006. (in Romanian)