Programming Research Group

A continuous domain of classical states

Keye Martin

PRG-RR-04-06

Oxford University Computing Laboratory
Wolfson Building, Parks Road, Oxford OX1 3QD

Abstract

We introduce an ω-continuous dcpo of classical states whose order is clearly demonstrable as a continuous form of logical implication. It has Shannon entropy as a measurement and can also be used to analyze Grover's algorithm for quantum searching. The fact that the n-simplex can be naturally given the structure of a *continuous* domain allows for the possibility of applying many well understood techniques in applications.

1 Introduction

In the fixed point characterization of entropy [7], a relation on the monotone decreasing subset Λ^n of classical states Δ^n emerges as a *qualitative* form of complexity. This relation, introduced by Muirhead[9] in 1903, is called *majorization.* It is well-known, ironically outside of domain theory, to be fundamental for many reasons ([2][6]). Only one hundred years after its introduction was it shown to form a continuous domain when restricted to Λ^n [7].

As far as we are aware, there is no clear way to extend majorization from Λ^n to all of Δ^n so that it retains all of its pleasing domain theoretic properties. However, there are good reasons to want a domain theoretic structure on Δ^n, and in [3], this problem is taken up and solved *with respect to ordering Δ^n so that it extends to quantum states that commute.* The relation on Δ^n defined there is called the *Bayesian order.* But the Bayesian order is *not continuous.*

Now, majorization has entropy as a measurement, and so does the Bayesian order. The first is a continuous domain but only on monotone states; the second is defined on all states but is discontinuous! It is more than just mathematical curiosity that leads us to ask whether or not it is possible to find a *continuous* domain of classical states with respect to which entropy is a measurement. Implicit in this is that we would like an order whose meaning is clear, and which can be used to do other things as well.

In this paper we prove that there is one, and show that the order is very clearly a continuous form of logical implication. We also use it to analyze Grover's algorithm for quantum searching. The real achievement is the discovery of an *understandable* and *ω-continuous* domain of classical states with respect to which entropy is a measurement. This provides an object that is part of traditional domain theory, one which we can now study using many well developed tools from the last thirty years, including ideas in the study of measurement [8].

2 Classical states

Let $\Delta^n = \{(x_1, \cdots, x_n) \in [0,1]^n : x_1 + \cdots + x_n = 1\}$ be the classical states in $n \geq 2$ dimensions. Set

$$x^+ = \max_{1 \leq i \leq n} x_i,$$

and

$$x^- = \min_{1 \leq i \leq n} x_i.$$

A state $x \in \Delta^n$ is *pure* if $x^+ = 1$. Δ^n has exactly n pure states $\{e_i : 1 \leq i \leq n\}$ which geometrically are the vertices of the n-simplex. The unique state $x \in \Delta^n$ with $x^+ = x^-$ is denoted $\perp$ and called the *completely mixed state.* The *monotone* decreasing states are

$$\Lambda^n := \{x \in \Delta^n : (\forall i < n)\, x_i \geq x_{i+1}\}$$

3 Domain theory

Let $(P, \sqsubseteq)$ be a partially ordered set or *poset* [1]. A nonempty subset $S \subseteq P$ is *directed* if $(\forall x, y \in S)(\exists z \in S)\, x, y \sqsubseteq z$. The *supremum* $\bigsqcup S$ of $S \subseteq P$ is the least of its upper bounds when it exists. A *dcpo* is a poset in which every directed set has a supremum.

For elements x, y of a dcpo D, we write $x \ll y$ iff for every directed subset S with $y \sqsubseteq \bigsqcup S$, we have $x \sqsubseteq s$, for some $s \in S$.

Definition 3.1 Let $(D, \sqsubseteq)$ be a dcpo. We set

- $\twoheaddownarrow x := \{y \in D : y \ll x\}$ and $\twoheaduparrow x := \{y \in D : x \ll y\}$
- $\downarrow x := \{y \in D : y \sqsubseteq x\}$ and $\uparrow x := \{y \in D : x \sqsubseteq y\}$

and say D is *continuous* if $\twoheaddownarrow x$ is directed with supremum x for each $x \in D$. A *domain* is a continuous dcpo.

The *Scott topology* on a domain D has as a basis all sets of the form $\twoheaduparrow x$ for $x \in D$. A function $f : D \to E$ between domains is *Scott continuous* if it reflects Scott open sets. This is equivalent to saying that f is *monotone,*

$$(\forall x, y \in D)\, x \sqsubseteq y \Rightarrow f(x) \sqsubseteq f(y),$$

and that it *preserves directed suprema*:

$$f(\bigsqcup S) = \bigsqcup f(S),$$

for all directed $S \subseteq D$.

Definition 3.2 A subset B of a dcpo D is a *basis* for D if $B \cap \twoheaddownarrow x$ contains a directed subset with supremum x, for each $x \in D$. A dcpo is *ω-continuous* if it has a countable basis.

Definition 3.3 For a poset P, P^* is the poset whose order is $x \sqsubseteq y \equiv y \sqsubseteq_P x$.

4 A continuous dcpo of classical states

Each $p \in [0,1]$ determines a poset $[0,1]_p$, which is the set $[0,1]$ with the order $\leq_p$ defined

$$x \leq_p y \Leftrightarrow y \leq x \leq p \text{ or } p \leq x \leq y.$$

Notice that $[0,1]_0 = [0,1]$ and $[0,1]_1 = [0,1]^*$.

Definition 4.1 *For $x, y \in \Delta^n$, we define*

$$x \sqsubseteq y \equiv (\forall i \in \{1, \ldots, n\})\, x_i \leq_p y_i$$

where $p = x^+$.

Lemma 4.2 *For $x, y \in \Delta^n$,*

$$x \sqsubseteq y \Rightarrow x^+ \leq y^+,$$

with equality iff $x = y$.

Proof. If $x_i \leq y_i$ for some i with $x_i = x^+$, then $x^+ \leq y_i \leq y^+$, and we are done. Thus, suppose $x_i > y_i$ for all i with $x_i = x^+$. Since $x \sqsubseteq y$, we have $x_i \geq y_i$ for $x_i \neq x^+$, which gives

$$1 = \sum_{x_i \neq x^+} x_i + \sum_{x_i = x^+} x_i > \sum_{i=1}^{n} y_i = 1.$$

Thus, $x^+ \leq y^+$.

Now suppose $x^+ = y^+$. First we argue that $x_i \geq y_i$. This is clear if $x_i \neq x^+$ since $x \sqsubseteq y$. If, on the other hand, $x_i = x^+$, then

$$x_i < y_i \Rightarrow x_i = x^+ < y_i \leq y^+,$$

which stands in contrast to $x^+ = y^+$. Because $x_i \geq y_i$, we have a series of nonnegative reals which sum to zero:

$$\sum_{i=1}^{n} (x_i - y_i) = 0.$$

Hence, $x_i - y_i = 0$ for all i. $\square$

Lemma 4.3 *Δ^n is a partially ordered set. Its maximal elements are the pure states*

$$\max(\Delta^n) = \{x \in \Delta^n : x^+ = 1\},$$

and its least element is the completely mixed state $\perp = (1/n, \cdots, 1/n)$.

Proof. Its reflexivity is obvious. For antisymmetry, if $x \sqsubseteq y$ and $y \sqsubseteq x$, then $x^+ \leq y^+$ and $y^+ \leq x^+$, so we have

$$x_i \leq_p y_i \ \& \ y_i \leq_p x_i$$

for all i where $p = x^+ = y^+$. By the antisymmetry of $\leq_p$, $x = y$.

For transitivity, let $x \sqsubseteq y$ and $y \sqsubseteq z$, and suppose $p = x^+$ and $q = y^+$. Then since $p \leq q$, we claim

$$x_i \leq_p y_i \ \& \ y_i \leq_q z_i \Rightarrow x_i \leq_p z_i.$$

To see why, consider two cases: Either $x_i = p$ or $x_i \neq p$. In the former, $x_i = p \leq_p z_i$. For the latter, $x_i < p = x^+$, which means

$$x_i \leq_p y_i \Rightarrow y_i \leq x_i < p \leq q,$$

and since $y_i < q$,

$$y_i \leq_q z_i \Rightarrow z_i \leq y_i,$$

which means $x_i \leq_p z_i$.

We have $\perp \sqsubseteq x$ because $1/n \leq_p x_i$ for $p = 1/n$.

For the maximal elements, suppose $x \in \max(\Delta^n)$. Let i be any index with $x_i = x^+$. Then it is clear that $x \sqsubseteq e_i$ where e_i is the pure state having a one at index i. By maximality of x, $x = e_i$.

Conversely, if $x^+ = 1$, and $x \sqsubseteq y$, then

$$x_i \leq_1 y_i.$$

But in the 1-order, $x_i = 0$ is maximal, which means $y_i = 0$ whenever $x_i = 0$. Then $x = y$ since they agree at all except one index. $\square$

For the remaining proofs, we need a simpler characterization of the order. We will often use the following result implicitly:

Lemma 4.4 *For $x, y \in \Delta^n$, $x \sqsubseteq y$ iff for all $i \in \{1, \ldots, n\}$, $x_i \geq y_i$ or $x_i = x^+$.*

We use the projections $\pi_k(x) = x_k$ defined on Δ^n for each $1 \leq k \leq n$.

Proposition 4.5 *Δ^n is a dcpo.*

Proof. All we need to do is prove that each increasing sequence has a supremum preserved by $f : \Delta^n \to [0,1] :: x \mapsto x^+$ and then appeal to its strict monotonicity in Lemma 4.2 to finish the proof. The supremum of a sequence (x_k) is

$$(\lim_{k\to\infty} \pi_1(x_k), \ldots, \lim_{k\to\infty} \pi_n(x_k)).$$

Each has a limit in the Euclidean topology because each is either increasing or eventually decreasing. $\square$

Δ^n can viewed as a continuous extension of $\mathcal{P}\{1, \ldots, n\}$, which will see in the next section. With this in mind, we call the *cardinality* of $x \in \Delta^n$

$$|x| := \mathrm{card}(\{i : x_i = x^+\}).$$

Theorem 4.6 *Δ^n is a continuous dcpo.*

Proof. For a given $x \in \Delta^n$, we construct an increasing sequence of approximations whose supremum is x. We can assume $x \neq \perp$. For any $\varepsilon > 0$ with

$$0 < \varepsilon \leq m := \min\{\ |x| \cdot x^+, (n - |x|)(1 - x^-)\ \}$$

we define a state x_ε by

$$(x_\varepsilon)_i := \begin{cases} x_i - \frac{\varepsilon}{|x|} & \text{if } x_i = x^+; \\ x_i + \frac{\varepsilon}{n-|x|} & \text{if } x_i \neq x^+. \end{cases}$$

Then $x_\varepsilon \ll x$ in Δ^n. If (ε_n) is a decreasing sequence with $0 < \varepsilon_n \leq m$ and $\varepsilon_n \to 0$, then (x_{ε_n}) is an increasing sequence in $\mathord{\downarrow\!\!\downarrow} x$ whose supremum is x. This proves Δ^n is continuous. $\square$

5 Implication

We now will show that $(\Delta^n, \sqsubseteq)$ can be viewed as a continuous extension of $\mathcal{P}\{1, \ldots, n\}$. First, we explain how $\mathcal{P}\{1, \ldots, n\}$ resides in Δ^n

Definition 5.1 An element x of a dcpo D is *irreducible* when

$$\bigwedge(\uparrow x \cap \max(D)) = x$$

The set of irreducible elements in D is written $\mathrm{Ir}(D)$.

Lemma 5.2 *For $x \in \Delta^n$, $x \sqsubseteq e_i$ iff $x_i = x^+$.*

Proof. Let $x \sqsubseteq e_i$. Then $x_i \geq 1$ or $x_i = x^+$. Either way, $x_i = x^+$. The other direction is clear. $\square$

Proposition 5.3 *For each $n \geq 2$, $\mathrm{Ir}(\Delta^n) \simeq (\mathcal{P}\{1, \ldots, n\} \setminus \{\emptyset\}, \supseteq)$.*

Proof. We will prove that

$$\mathrm{Ir}(\Delta^n) = \{p \in \Delta^n : (\forall i)\, p_i = p^+ \text{ or } p_i = 0\}$$

from which the claim is immediate. First, let $x \in \mathrm{Ir}(\Delta^n)$. Then $x = \bigwedge X$ for $\emptyset \neq X \subseteq \max(\Delta^n)$. Let $p \in \Delta^n$ be the unique state such that $p_i = p^+$ iff $e_i \in X$ and $p_i = 0$ otherwise. Then p is a lower bound for X. If u is any other lower bound for X, then for $u_i \neq u^+$, we know that $e_i \notin X$, which means $p_i = 0$ and hence $u_i \geq p_i$. Then $u \sqsubseteq p$. This proves $p = \bigwedge X = x$.

Conversely, let $p \in \Delta^n$ have the property that either $p_i = p^+$ or $p_i = 0$. By Lemma 5.2, $\uparrow p \cap \max(\Delta^n) = \{e_i : p_i = p^+\}$. Now borrowing the argument of the previous direction proves $p = \bigwedge(\uparrow p \cap \max(\Delta^n))$. $\square$

Now we explain how Δ^n is a continuous extension of $\mathcal{P}\{1, \ldots, n\}$. First, each set $A \in \mathcal{P}\{1, \ldots, n\}$ has a characteristic function $\chi_A : \{1, \ldots, n\} \to \{0, 1\}$ defined by

$$\chi_A(i) := \begin{cases} 1 & \text{if } i \in A; \\ 0 & \text{otherwise.} \end{cases}$$

We then have

$$A \supseteq B \iff \chi_A \geq \chi_B$$

where $\geq$ is the pointwise order on functions of type $\{1, \ldots, n\} \to \{0, 1\}$ and $1 \geq 0$. But each $A \in \mathcal{P}\{1, \ldots, n\} \setminus \{\emptyset\}$ corresponds to a canonical classical state $x \in \mathrm{Ir}(\Delta^n)$ given by

$$x_i := \begin{cases} x^+ & \text{if } i \in A; \\ 0 & \text{otherwise,} \end{cases}$$

so we can also think of x as having a characteristic function

$$\chi_x : \{1, \ldots, n\} \to [0, 1]$$

given by

$$\chi_x(i) := \begin{cases} 1 & \text{if } x_i = x^+; \\ x_i & \text{otherwise.} \end{cases}$$

But this definition makes sense *for any* classical state $x \in \Delta^n$.

Theorem 5.4 *For $x, y \in \Delta^n$, $x \sqsubseteq y$ if and only if $\chi_x \geq \chi_y$.*

Proof. Let $x \sqsubseteq y$. If $x_i = x^+$, then $\chi_x(i) = 1 \geq \chi_y(i)$. Otherwise, $x_i \neq x^+$. Then $\chi_x(i) = x_i$. But we also know $y_i \neq y^+$: if not, we would have $x \sqsubseteq y \sqsubseteq e_i$, and thus $x_i = x^+$ by Lemma 5.2. Then $\chi_y(i) = y_i$. By Lemma 4.4, $\chi_x(i) = x_i \geq \chi_y(i) = y_i$. This proves $\chi_x \geq \chi_y$.

Conversely, suppose $\chi_x \geq \chi_y$. Assume $x_i \neq x^+$. Then $\chi_x(i) = x_i$. If $\chi_y(i) = 1$, then $\chi_x(i) = x_i \geq \chi_y(i) = 1$, which contradicts $x_i \neq x^+$. Then $\chi_y(i) = y_i$, and since $\chi_x \geq \chi_y$, we must have $\chi_x(i) = x_i \geq \chi_y(i) = y_i$. By Lemma 4.4, we have proven $x \sqsubseteq y$. $\square$

Then the order can legitimately be called implication of states, and we name it the *implicative* order. Understanding $(\Delta^n, \sqsubseteq)$ as a continuous form of implication is the crucial idea in proving certain functions are measurements on Δ^n.

6 Measurement

Definition 6.1 A Scott continuous map $\mu : D \to E$ between domains *measures* the elements in a set $X \subseteq D$ if for all $x \in X$ and for all Scott open $U \subseteq D$,

$$x \in U \Rightarrow (\exists\, \varepsilon \in E)\, x \in \mu_\varepsilon(x) \subseteq U$$

where $\mu_\varepsilon(x) := \{y \in D : y \sqsubseteq x \;\&\; \varepsilon \ll \mu y\}$ are the ε-*approximations* of $x \in D$.

In this paper, we will usually have $E = [0, \infty)^*$, the set of nonnegative reals in their reverse order, so μ will be a measure of uncertainty. In this case μ will measure $X \subseteq D$ if for all $x \in X$ and for all Scott open $U \subseteq D$,

$$x \in U \Rightarrow (\exists\, \varepsilon > 0)\, x \in \mu_\varepsilon(x) \subseteq U$$

where for convenience in this case we redefine the ε-approximations of x to be

$$\mu_\varepsilon(x) := \{y \in D : y \sqsubseteq x \ \&\ |\mu x - \mu y| < \varepsilon\}$$

for $\varepsilon > 0$.

Definition 6.2 A *measurement* is a Scott continuous map $\mu : D \to [0, \infty)^*$ that measures $\ker \mu := \{x \in D : \mu x = 0\}$.

A map $\mu : D \to E$ that measures D is *strictly monotone*:

$$(\forall x, y \in D)\, x \sqsubseteq y \ \&\ \mu x = \mu y \Rightarrow x = y.$$

A continuous embedding $e : D \to E$ is an important example of a map that measures D. To illustrate, by Theorem 5.4, there is a continuous embedding from the implicative order to the product of n copies of $[0, 1]^*$

$$\Delta^n \longrightarrow \prod_{i=1}^{n} [0, 1]^*$$

Maps that measure their entire domains are closed under composition. We now use these facts as follows:

Lemma 6.3 *The map* $f(x) = (1 - x^+) \cdot |x|$ *measures* Δ^n.

Proof. We use the embedding of Δ^n into $\prod_{i=1}^n [0, 1]^*$. If m measures $[0, 1]^*$, then

$$g(x) = \sum_{x_i \neq x^+} m(x_i) + \sum_{x_i = x^+} m(1)$$

measures Δ^n. Then, if we take m to be the identity map on $[0, 1]^*$,

$$g(x) = \left(\sum_{x_i \neq x^+} x_i \right) + |x|$$

measures Δ^n. Since $|x| \geq 1$, $f(x) = g(x) - 1 \geq 0$ and also measures Δ^n. But

$$f(x) = (1 - |x| \cdot x^+ + |x|) - 1 = (1 - x^+) \cdot |x|$$

which finishes the proof. $\Box$

But cardinality is locally constant:

Lemma 6.4 *Given $x \in \Delta^n$, there is $\varepsilon > 0$ such that*

$$a \sqsubseteq x \ \& \ |a^+ - x^+| < \varepsilon \Rightarrow |a| = |x|.$$

Proof. If not, for each $k \geq 1$, there is $a_k \sqsubseteq x$ with $|a_k^+ - x^+| < 1/k$ and $|a_k| > |x|$. Let $S := \{i : x_i = x^+\}$. There is $j \in \{1, \ldots, n\} \setminus S$ such that $(\pi_j(a_k))_{k \geq 1}$ contains an infinite subsequence $(\pi_j(a_{k_i}))_{i \geq 1}$ with $\pi_j(a_{k_i}) = a_{k_i}^+$ for each $i \geq 1$. (Otherwise, we could prove that for large enough k, $|a_k| = |x|$.)

We can assume (a_{k_i}) has the following property: For any $j \notin S$, if $\pi_j(a_{k_i}) = a_{k_i}^+$ for *some* i, then

(i) For *all* $i \geq 1$, $\pi_j(a_{k_i}) = a_{k_i}^+$, and

(ii) $\lim_{i \to \infty} \pi_j(a_{k_i}) = x^+ > x_j$.

First, we know that one such j does exist, and for this j, the limit in (ii) exists since (a_k) converges to x^+. If the inequality in (ii) failed, we would have $x^+ \leq x_j$ hence $x_j = x^+$ which puts $j \in S$, a contradiction. By taking subsequences of (a_{k_i}) if necessary, we can assume all the same about any other such $j \notin S$.

Now let $j \notin S$ satisfy $\pi_j(a_{k_i}) = a_{k_i}^+$. There is K such that for all $i \geq K$,

$$0 \leq \sum_{m \in S} (x^+ - \pi_m(a_{k_i})) < \pi_j(a_{k_i}) - x_j.$$

First, the sum is nonnegative: $a_{k_i} \sqsubseteq x$ and $x_m = x^+$ implies $\pi_m(a_{k_i}) = a_{k_i}^+ \leq x^+$. Next, the strict inequality on the right is achievable because the sum tends to zero while $\pi_j(a_{k_i}) - x_j$ tends to $x^+ - x_j > 0$ as $i \to \infty$. Then for $i \geq K$,

$$\sum_{m \in S \cup \{j\}} \pi_m(a_{k_i}) \ > \sum_{m \in S \cup \{j\}} x_m. \tag{1}$$

Now consider $m \in S \cup \{j\}$. If $\pi_m(a_{k_i}) \neq a_{k_i}^+$, then $\pi_m(a_{k_i}) \geq x_m$ since $a_{k_i} \sqsubseteq x$; otherwise, by (ii), for large enough i, $\pi_m(a_{k_i}) \geq x_m$. Thus, we can find L such that for $i \geq L$,

$$\sum_{m \notin S \cup \{j\}} \pi_m(a_{k_i}) \ \geq \sum_{m \notin S \cup \{j\}} x_m. \tag{2}$$

Then for $i \geq \max\{K, L\}$, both (1) and (2) hold, which implies that

$$\sum_{m=1}^{n} \pi_m(a_{k_i})) > 1$$

which is (finally!) a contradiction. □

Now we have our first example of a natural measurement:

Lemma 6.5 *The map $u(x) = 1 - x^+$ measures Δ^n.*

Proof. This is a trivial but satisfying exercise. Let $U \subseteq \Delta^n$ be a Scott open set with $x \in U$. By Lemma 6.3, there is $\delta > 0$ such that

$$y \sqsubseteq x \;\&\; |f(x) - f(y)| < \delta \;\Rightarrow\; y \in U.$$

By Lemma 6.4, there is $\alpha > 0$ such that

$$y \sqsubseteq x \;\&\; |x^+ - y^+| < \alpha \;\Rightarrow\; |x| = |y|.$$

Let $\varepsilon > 0$ satisfy $\varepsilon < \min\{\delta/|x|, \alpha\}$ and suppose

$$y \sqsubseteq x \;\&\; |u(x) - u(y)| < \varepsilon.$$

We will prove that $y \in U$. First, since $|x^+ - y^+| < \varepsilon < \alpha$, $|x| = |y|$. Next,

$$|f(x) - f(y)| = |x| \cdot |x^+ - y^+| < |x| \cdot \varepsilon < |x| \cdot \frac{\delta}{|x|} = \delta$$

which gives $y \in U$. $\square$

We are now in a position to give a clean proof of the following:

Proposition 6.6 *Δ^n is an ω-continuous dcpo.*

Proof. We prove that each $x \in \Delta^n$ is the sup of an increasing sequence in

$$B := \{x \in \Delta^n : x_i \in \mathbb{Q}\}.$$

Since this is true for $x = \perp$, we assume $x \neq \perp$. Then from $x^+ > 1/n$, we know

$$\delta := \frac{1}{n - |x|} \cdot \left(\left(1 - \frac{1}{n}\right) - \sum_{x_i \neq x^+} x_i \right) > 0$$

so let $\varepsilon > 0$ be arbitrary and set $\alpha := \min\{\delta, \varepsilon\} > 0$. For each $x_i \neq x^+$, choose a rational $r_i \in \mathbb{Q}$ such that $r_i > x_i$ & $0 < r_i - x_i < \alpha$. First,

$$0 \;\leq\; \sum_{x_i \neq x^+} (r_i - x_i) \;<\; \alpha \cdot (n - |x|) \;\leq\; \delta \cdot (n - |x|) \;=\; \left(1 - \frac{1}{n}\right) - \sum_{x_i \neq x^+} x_i$$

which immediately gives

$$0 \leq \sum_{x_i \neq x^+} r_i < \left(1 - \frac{1}{n}\right) \leq 1.$$

Thus, for $x_i = x^+$, we can define

$$r_i := \frac{1}{|x|} \left(1 - \sum_{x_i \neq x^+} r_i\right) \in \mathbb{Q}.$$

Then for any $\varepsilon > 0$, $r = (r_1, \ldots, r_n) \in B$, $r \ll x$ and $|r_i - x_i| < \varepsilon$ for each i. This proves that $\downarrow x$ contains a sequence (a_n) with $a_n \in B$ and $u(a_n) \to u(x)$. Since u measures Δ^n, the sequence (a_n) must be directed, and thus have supremum x. This proves B is a countable basis for Δ^n. $\Box$

Later, we will find the following measurement very useful:

Lemma 6.7 *The map $v(x) = 1 - \sqrt{x^+}$ measures Δ^n.*

Proof. To prove this, we have to consider $y \in U$ and $x \sqsubseteq y$, and show that $x \in U$ provided $|v(x) - v(y)|$ is small enough. By the mean value theorem, applied to $\sqrt{t}$ on $[x^+, y^+]$, there is $c \in (x^+, y^+)$ with

$$|\sqrt{x^+} - \sqrt{y^+}| \;=\; \frac{1}{2\sqrt{c}}|x^+ - y^+| \;\geq\; \frac{1}{2}|x^+ - y^+|,$$

where the inequality is from $c \leq x^+ \leq 1$. Then, if we make $|\sqrt{x^+} - \sqrt{y^+}|$ small we also make $|x^+ - y^+|$ small. Since $u(x) = 1 - x^+$ measures Δ^n, so does v. $\Box$

In a similar way, $s(x) = -\log x^+$ also measures Δ^n. Finally, we briefly consider Shannon entropy

$$\mu x = -\sum_{i=1}^{n} x_i \log x_i$$

which defines a Euclidean continuous function from Δ^n to $[0, \infty)^*$. By convention, $0 \log 0 = 0$.

Theorem 6.8 *Shannon entropy $\mu : \Delta^n \to [0, \infty)^*$ is a strictly monotone measurement with* $\ker \mu = \max(\Delta^n)$.

Proof. First the monotonicity. Let $x \sqsubseteq y$. First we partition $\{1, \ldots, n\}$ into the union of pairwise disjoint sets X_1, X_2, X_3 as $\{1, \ldots, n\} = X_1 \cup X_2 \cup X_3$ where

$$X_1 = \{i : x_i = x^+ \;\&\; x_i \leq y_i\},$$

$$X_2 = \{i : x_i = x^+ \;\&\; x_i > y_i\}, \quad X_3 = \{i : x_i \neq x^+\}.$$

Let $\sigma : \{1, \ldots, n\} \to \{1, \ldots, n\}$ be a bijection with $x \cdot \sigma : \{1, \ldots, n\} \to [0, 1]$ in Λ^n, $\sigma\{1, \ldots, |X_1|\} \subseteq X_1$, $\sigma\{|X_1| + 1, \ldots, |X_1| + |X_2|\} \subseteq X_2$, and $\sigma\{|X_1| + |X_2| + 1, \ldots, n\} \subseteq X_3$.

Since $\mu(x \cdot \sigma) = \mu x$ and $\mu(y \cdot \sigma) = \mu y$, we can assume (by choosing a permutation σ if necessary) that $x \in \Lambda^n$ and that there is $k \in \{1, \ldots, n\}$ such that $x_i \leq y_i$ for $i < k$ and $x_i \geq y_i$ for $i \geq k$. Then

$$\sum_{i=1}^{n} (y_i - x_i) \log x_i = \sum_{i<k} (y_i - x_i) \log(x_i / x_k) + \sum_{i>k} (y_i - x_i) \log(x_i / x_k) \geq 0.$$

Notice that if $x_k = 0$, then $x_i = 0 \geq y_i$ for $i > k$ since $x \in \Lambda^n$, which means the sum of the $i > k$ vanishes, while the sum of the $i < k$ blows up, but is nevertheless nonnegative. From the nonnegativity of this sum, we have

$$\mu x \geq -\sum_{i=1}^{n} y_i \log x_i \geq \mu y,$$

where the second inequality follows from the fact we always have

$$\mu(y\|x) := \sum_{i=1}^{n} y_i \log(y_i/x_i) \geq 0.$$

This proves that μ is monotone into $[0,\infty)^*$.

If in addition to $x \sqsubseteq y$ we also have $\mu x = \mu y$, then the inequality above immediately gives $\mu(y\|x) = 0$, which implies $x = y$. This establishes that μ is strictly monotone. For its Scott continuity, if (x_i) is increasing, then

$$\begin{aligned} \mu(\bigsqcup x_i) &= \mu(\lim_{i\to\infty} \pi_1(x_i), \ldots, \lim_{i\to\infty} \pi_n(x_i)) \\ &= \lim_{i\to\infty} \mu(\pi_1(x_i), \ldots, \pi_n(x_i)) \\ &= \lim_{i\to\infty} \mu x_i, \end{aligned}$$

where the first equality uses the fact that suprema are calculated using Euclidean limits and the second uses the continuity of μ with respect to the Euclidean topology. Then μ is Scott continuous. Finally, μ is a measurement: For $x \in \Delta^n$, we have

$$\mu x \geq -x^+ \log x^+ \geq \frac{1}{n} \cdot u(x),$$

using $\log t \leq t - 1$ for $t > 0$ and $x^+ \geq 1/n$, where $u(x) = 1 - x^+$ is the measurement from earlier. Since u is a measurement, $(1/n) \cdot u$ is a measurement, which means that μ is as well. ☐

Space constraints have prevented us from considering the interesting question of whether μ measures Δ^n with respect to implication.

7 Quantum searching

Grover's algorithm [4] for searching is the only known quantum algorithm whose complexity is *provably better* than its classical counterpart. We will now use the implicative order to analyze this algorithm. Here are some crucial things the approach yields:

(a) The complexity of the algorithm,

(b) A qualitative property the algorithm possesses called *antimonotonicity.* Without knowledge of this aspect, an experimental implementation would almost certainly fail (for reasons that will be clear later).

(c) An explanation of the algorithm as being an attempt to calculate a classical proposition.

Grover's algorithm searches a list L of length n (a power of two) for an element k known to occur in L precisely m times with $n > m \geq 1$. The register begins in the pure state

$$|\psi\rangle = \frac{1}{\sqrt{n}} \sum_{i=1}^{n} |i\rangle$$

and after j iterations of the Grover operator G

$$G^j|\psi\rangle = \frac{\sin(2j\theta + \theta)}{\sqrt{m}} \sum_{L(i)=k} |i\rangle + \frac{\cos(2j\theta + \theta)}{\sqrt{n-m}} \sum_{L(i)\neq k} |i\rangle$$

where $\sin^2 \theta = m/n$. The probability that a measurement yields i after j iterations is

$$\sin^2(2j\theta + \theta)/m \text{ if } L(i) = k$$

and

$$\cos^2(2j\theta + \theta)/(n-m) \text{ if } L(i) \neq k.$$

To get the answer, we measure the state of the register in the basis $\{|i\rangle : 1 \leq i \leq n\}$; if we perform this measurement after j iterations of G, when the state of the register is $G^j|\psi\rangle$, our knowledge about the result is represented by the classical state

$$x(j) = \left(\frac{\sin^2(2j\theta + \theta)}{m}, \ldots, \frac{\sin^2(2j\theta + \theta)}{m}, \frac{\cos^2(2j\theta + \theta)}{n-m}, \ldots, \frac{\cos^2(2j\theta + \theta)}{n-m} \right)$$

The crucial step now is to *imagine* t iterations,

$$x(t) = \left(\frac{\sin^2(2t\theta + \theta)}{m}, \ldots, \frac{\sin^2(2t\theta + \theta)}{m}, \frac{\cos^2(2t\theta + \theta)}{n-m}, \ldots, \frac{\cos^2(2t\theta + \theta)}{n-m} \right)$$

which defines a monotone state for $t \in \mathrm{dom}(x) = [a, b]$, $a = 0$ and $b = \pi/2\theta - 1$. The image of $x : [a, b] \to \Lambda^n$ is a chain in the implicative order, which is simplest to see by noting that it has the form

$$x = (f, \ldots, f, g, \ldots, g)$$

so that $g(s) \geq g(t) \Rightarrow x(s) \sqsubseteq x(t)$; otherwise, $x(t) \sqsubseteq x(s)$. We can now determine the exact nature of the motion represented by x with the following observation: If $x : [a, b] \to D$ is a curve on a domain D whose image is a chain and whose time derivative

$$\dot{x}_v(t) := \frac{d(v \circ x)}{dt}(t) = \lim_{s \to t} \frac{vx(s) - vx(t)}{s - t}$$

exists with respect to a strictly monotone measurement v on Δ^n, then

(i) The curve x has an absolute maximum on $[a, b]$: There is $t^* \in [a, b]$ such that

$$x(t^*) = \bigsqcup_{t \in [a,b]} x(t),$$

and

(ii) Either $t^* = a$, $t^* = b$ or $\dot{x}_v(t^*) = 0$.

Part of the power of this simple approach is that we are free to choose any v we like. To illustrate, a tempting choice might be entropy $v = \mu$, but then solving $\dot{x}_v = 0$ means solving the equation

$$-m\dot{f}(1 + \log f) - (n - m)\dot{g}(1 + \log g) = 0$$

and we also have to determine the points where $\dot{x}_v$ is undefined, the set $\{t : g(t) = 0\}$. However, if we use the measurement

$$v = 1 - \sqrt{x^+},$$

we only have to solve a single elementary equation

$$\cos(2t\theta + \theta) = 0$$

for t, allowing us to conclude that the maximum must occur at $t = a$, $t = b$, or at points in

$$\{t : \dot{x}_v(t) = 0\} = \{b/2\}.$$

The absolute maximum of x is

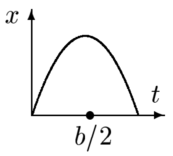
$$x(b/2) = (1/m, \ldots, 1/m, 0, \ldots, 0)$$

because for the other points we find a minimum of

$$x(a) = x(b) = \perp.$$

The value of knowing the absolute maximum is that it allows us to calculate the complexity of the algorithm: It is $O(b/2)$, the amount of time required to move to a state from which the likelihood of obtaining a correct result by measurement is maximized. This gives $O(\sqrt{n/m})$ using $\theta \geq \sin\theta \geq \sqrt{m/n}$ and then $b/2 \leq (\pi/4)\sqrt{n/m} - 1/2$.

From $\dot{x}_v(t) \leq 0$ on $[a, b/2]$ and $\dot{x}_v(t) \geq 0$ on $[b/2, b]$, we can also graph x:



This is the 'antimonotonicity' of Grover's algorithm: If $j = b/2$ iterations will solve the problem accurately, $2j$ iterations will mostly unsolve it! This means that our usual way of reasoning about iterative procedures like numerical methods, as in "we must do at least j iterations," no longer applies. We must say "do exactly j iterations; no more, no less." As is now clear, precise estimates like these have to be obtained before going into a laboratory whenever possible.

Finally, we can view Grover's algorithm as an attempt to calculate as closely as possible the classical proposition

$$x(b/2) = (1/m, \ldots, 1/m, 0, \ldots, 0) \in \mathrm{Ir}(\Delta^n).$$

It does so by generating *approximations*

$$x(t) \ll x(b/2)$$

for all $t \neq b/2$.

8 Distance

Before leaving, we want to give an example of the specific value there is in knowing that a map $\mu : \Delta^n \to [0,\infty)^*$ measures Δ^n with respect to the implicative order. First, we can define

$$d(x,y) = \inf\{\mu z : z \sqsubseteq x, y\}$$

which is Scott continuous from $\Delta^n \times \Delta^n$ to $[0,\infty)^*$. But *because Δ^n is continuous,* the sets

$$B_\varepsilon(x) = \{y \in \Delta^n : d(x,y) < \varepsilon\}$$

form a basis for the Scott topology on Δ^n. In addition,

$$d(x,y) = \max\{\mu x, \mu y\} \;\Leftrightarrow\; (x \sqsubseteq y \text{ or } y \sqsubseteq x).$$

For example, Grover's trajectory $x : [a,b] \to \Delta^n$ satisfies

$$d(x(s), x(t)) = \max\{\mu x(s), \mu x(t)\}$$

for all $s, t \in [a,b]$ because its image is a chain.

9 Closing

Both the Bayesian order and the implicative order when restricted to Λ^n are contained in majorization. What distinguishes each of them from majorization though is that they are defined on all of Δ^n as opposed to only Λ^n, and as we have seen, if we throw out permutations of states, we also throw out the ability to interpret classical states as continuous extensions of classical propositions. The implicative order is not contained in the Bayesian order, or vice-versa.

The feature of the implicative order that distinguishes it from the Bayesian order is that the former is *continuous.* The Bayesian order's crucial property is that it extends to quantum states which commute. The implicative order does not seem to have this property. However, if we restrict the implicative order $\sqsubseteq$ to a smaller order $\leq$ defined by

$$x \leq y \Leftrightarrow x \sqsubseteq y \;\&\; ((y_i = y_j > 0) \Rightarrow (x_i = x_j > 0)),$$

then $\leq$ will extend to commutative quantum states (but will not be continuous). It might be possible to leave the implicative order alone and instead restrict the order on quantum states, by requiring not only that they commute, but some additional requirement. The key issue with quantum states is ensuring transitivity. A completely new approach to quantum states would also be interesting.

We think the fact that the implicative order on Δ^n is continuous, natural and respected by entropy is very encouraging, and we are happy that a structure has finally been found which fits perfectly within the context of traditional domain theory and also seems likely to have many interesting uses in computer science, physics and economics. To illustrate a few ideas along this line, in quantum computation, any algorithm that respects the implicative order can immediately be seen (by its very definition) to be progressing in a decent way: the only probabilities which can increase are those which are maximum, all others decrease. This is not true for any other order that we are aware of. Thus, respecting the implicative order may be a property that quantum algorithms with 'good' complexities have. In economics, Brouwer's fixed point theorem on Δ^n is often used to demonstrate the existence of equilibria with the disadvantage that it does not yield an approach for calculating fixed points. It might be possible to alleviate this difficulty in some cases by using the implicative order on Δ^n and various fixed point theorems in domain theory.

References

[1] S. Abramsky and A. Jung. *Domain theory.* In S. Abramsky, D. M. Gabbay, T. S. E. Maibaum, editors, Handbook of Logic in Computer Science, vol. III. Oxford University Press, 1994.

[2] P. M. Alberti and A. Uhlmann. *Stochasticity and partial order: doubly stochastic maps and unitary mixing.* Dordrecht, Boston, 1982.

[3] B. Coecke and K. Martin. *A partial order on classical and quantum states.* Research Report PRG-RR-02-07, Oxford University Computing Laboratory, August 2002, `http://web.comlab.ox.ac.uk/oucl/publications/tr/rr-02-07.html`

[4] L. K. Grover. *Quantum mechanics helps in searching for a needle in a haystack.* Physical Review Letters, **78**:325, 1997.

[5] Latorre, J. I. and M. A. Martín-Delgado. *The majorization arrow in quantum algorithm design.* Physical Review A, **66**:022305, 2002.

[6] A. W. Marshall and I. Olkin. *Inequalities: Theory of majorization and its applications.* Academic Press Inc., 1979.

[7] K. Martin. *Entropy as a fixed point.* ICALP 2004, Lecture Notes in Computer Science, to appear.

[8] K. Martin. *The measurement process in domain theory.* ICALP 2000, Lecture Notes in Computer Science, vol. 1853, 2000.

[9] R. F. Muirhead. *Some methods applicable to identities and inequalities of symmetric algebraic functions of n letters.* Proc. Edinburgh Math. Soc., 21:144-157, 1903.