CSP PRIMER[2]

WILLIAM DEMEO

1. Preliminary Definitions and Notations

a. If A and B are sets, then the *Cartesian product* of A and B is denoted by $A \times B$ and is defined to be the set of all ordered pairs (a, b) such that a belongs to A and b belongs to B; that is,

$$A \times B = \{(a, b) : a \in A,\, b \in B\}.$$

If A is a set and n is a natural number, then the n-th *Cartesian power* of A, denoted by A^n, is the set of n-tuples of elements of A; that is,

$$A^n = A \times A \times \cdots \times A = \{(a_1, a_2, \ldots, a_n) : a_i \in A \text{ for } 1 \le i \le n\}.$$

If $|A|$ denotes the number of elements in the set A, then A^n contains exactly $n^{|A|}$ elements.

We define the *k-th projection on n-tuples* to be the function $\pi_k : A^n \to A$ given by

$$\pi_k(a_1, a_2, \ldots, a_n) = a_k.$$

That is, π_k simply projects onto the k-th "coordinate" of A^n by picking out the k-th entry of $(a_1, a_2, \ldots, a_n)$.

It is important to note that each n-tuple $(a_1, a_2, \ldots, a_n) \in A^n$ in the Cartesian power of A defines a function mapping the set $\{1, 2, \ldots, n\}$ to the set A. Specifically, $(a_1, a_2, \ldots, a_n)$ is the function $a : \{1, 2, \ldots, n\} \to A$ given by $a(k) = \pi_k(a_1, \ldots, a_n) = a_k$. It may seem like we're making something out of nothing here, but this slight change of viewpoint (tuples as functions) can be very useful. Thus, the Cartesian power A^n "is" the set of all funcitons from $\{1, 2, \ldots, n\}$ to A.

Exercise 1 (easy). *Use a counting principle to explain why there are $n^{|A|}$ elements in A^n.*

b. For two sets X and Y, we denote by Y^X the set of all functions $f : X \to Y$ that map each element $x \in X$ to some element $f(x) \in Y$. Take a moment to observe the analogy with tuples. Indeed, the function f is an $|X|$-tuple of elements of Y. This analogy is exact when X happens to be a countable set, in which case we can enumerate its elements, $X = \{x_1, x_2, \ldots\}$. This allows us to represent f by the tuple consisting of its values: $f = (f(x_1), f(x_2), \ldots)$, and applying f to an "index" $x_k \in X$ gives the k-th element in the tuple f:

$$f(x_k) = \pi_k(f(x_1), f(x_2), \ldots) = \pi_k f.$$

But the analogy with tuples is useful even when the domain is not countable and we may think of f as a "tuple" $(f(x) : x \in X) \in Y^X$. There is no harm in thinking of Y^X as a Cartesian

Date: 12 May 2015.

power in this case as well, as long as you don't make the mistake of assuming we can always enumerate the "index set" X. In particular, if X is an uncountable set, then you shouldn't write $(f(x_1), f(x_2), \dots)$ instead of $(f(x) : x \in X)$. That is, you cannot write the values of f as an enumerated list of elements of Y. There are simply too many values!

Exercise 2 (easy)**.** *If X has $|X| = m$ elements and Y has $|Y| = n$ elements, how many functions are there from X to Y? In other words, what is the cardinality of the set Y^X? How many of these functions are one-to-one? (Hint: handle the cases $m \le n$ and $m > n$ separately.)*

c. The k-th projection operation on n-tuples defined above has domain A^n and codomain A, so it belongs to the set $A^{(A^n)}$. Note that $A^{(A^n)}$ has the form Y^X described above; in this case $Y = A$ and $X = A^n$.

Unfortunately, we have to use a slightly uglier, but more precise, notation for projections. We let $\pi^n_k : A^n \to A$ denote the k-th projection on A^n, since we will occasionally refer to projections of other arities, say, $\pi^m_k : A^m \to A$ in the same context.

Let A be any set and let n be any natural number. Then $A^{(A^n)}$ denotes the set of all n-ary functions on A, that is, the set of all functions $f : A^n \to A$ taking an n-tuple $(a_1, \dots, a_n) \in A^n$ to some value $f(a_1, \dots, a_n) \in A$. In symbols,

$$A^{(A^n)} = \{f : A^n \to A\}$$

(You are probably familiar with such "multivariable" functions from calculus.) We let $\mathrm{Op}(A)$ denote the set of all functions from A^n to A for all natural numbers n. In symbols,

$$\mathrm{Op}(A) = \bigcup_{n \in \mathbb{N}} A^{(A^n)}.$$

d. Let n and k be natural numbers, and suppose that $f \in A^{(A^n)}$ and $g_1, g_2, \dots, g_n \in A^{(A^k)}$. Then we define a new k-ary operation $f[g_1, g_2, \dots, g_n]$ by

$$(a_1, a_2, \dots, a_k) \mapsto f(g_1(a_1, \dots, a_k), \dots, g_n(a_1, \dots, a_k))$$

called the *generalized composition* of f with $g_1, \dots, g_n$. Note that, unlike the ordinary composition of unary functions, the generalized composition exists only when the arities match up correctly.

Just as the set of unary operations forms a monoid[1] under the operation of composition, we can form an algebraic structure whose elements are members of $\mathrm{Op}(A)$ with the operation of generalized composition.

Definition 1. *Let A be a nonempty set. A* **clone** *on A is a subset $\mathscr{C}$ of $\mathrm{Op}(A)$ that contains all projection operations and is closed under generalized composition.*

Exercise 3. *Show that the set $\mathrm{Proj}(A)$ of all projections $\{\pi^n_k : n \in \mathbb{N},\ k \in \mathbb{N}\}$ on the set A is a clone.*

[1]A *monoid*, $\langle X, \circ, e\rangle$, is a set X together with an associative binary operation $\circ$ and an identity element e. Note that the set A^A of all unary functions $f : A \to A$, along with function composition $f \circ g$ and the identity map id_A, forms a monoid, $\langle A^A, \circ, \mathrm{id}_A\rangle$.

Exercise 4. *Show that the set $\mathcal{E}(A)$ of all* idempotent *operations on A is a clone. An operation f is called idempotent if $f(a, a, \ldots, a) = a$ for all $a \in A$.*

Given a set $F \subseteq \mathrm{Op}(A)$ of functions, we can consider the smallest clone that contains F. This is called the *clone generated by* F and is denoted by $\mathrm{Clo}(F)$. It is no too hard to prove that the clone $\mathrm{Clo}(F)$ can be built recursively, as in the following theorem:

Theorem 1. *Let A be a set and $F \subseteq \mathrm{Op}(A)$ a set of operations on A. Define*

$$F_0 = \mathrm{Proj}(A)$$
$$F_{n+1} = F_n \cup \{f[g_1, \ldots, g_k] : f \in F, k = \mathrm{arity}(f), g_1, \ldots, g_k \in F_n \cap \mathrm{Op}(A)\},$$

Then $\mathrm{Clo}(F) = \bigcup_n F_n$.