Computers, Formal Systems, and Simulations: Alluding to the Curry–Howard correspondence

Brian Tenneson

January 19, 2024

Graduate Student

Bay Path University

Department of Applied Data Science

btenneson2301@baypath.edu

Abstract

I discuss one possible formal definition of the word "computer" in the definition of semi-ideal computers or SICs for short. The notion of a SIC associated with a formal system and the formal system associated with a SIC implies a dictionary between the totality of all formal systems and all SICs, pointing to the the Curry–Howard correspondence. Simulations are then discussed in terms of labeled state transitions, including a mention of what I call a depth m simulation of a SIC. I will proceed to develop a definition of an automated theorem prover to be an effective SIC, meaning that the ATP can prove all provable theorems.

Keywords: computer, formal system, simulation, the Curry–Howard correspondence, semi-ideal computer, automated theorem prover

Disclaimer: Opinions and conclusions reached in this document are not necessarily representative of Bay Path University.

1 Definitions

To fix notation, $\mathbb{F}_m = \mathbb{N} \cap [1, m]$. $[a \to b]$ denotes the set of all functions whose domain is a and codomain is b. $|x|$ is the cardinal number of set x. $f[a] = \{f(a) : a \in A\}$.

Definition $F = (x, y, z)$ is an xyz **formal system** if

1. x is nonempty,
2. $y \subseteq \bigcup_{m=1}^{\infty} [\mathbb{F}_m \to x]$, and
3. $z \subseteq \bigcup_{m=1}^{\infty} \bigcup_{G \in \mathcal{P}(y^m)} [G \to y]$.

Elements of x will be called **symbols**; x is referred to as an **alphabet**. Elements of y are **well-formed formulas**. Elements of z are **inference rules**. Note that, for each $m \geq 1$, $[\mathbb{F}_m \to x]$ is the set of all length m sequences of elements of x, sometimes called **strings** or **utterances**. The utterances in y are deemed to be well-formed.

Note the two following facts stemming from this definition:

1. $w \in y$ implies $(\exists m \geq 1)\,(w \in [\mathbb{F}_m \to x])$;
2. $i \in z$ implies $(\exists m \geq 1)\,(\exists G \subseteq y^m)\,(i \in [G \to y])$.

All elements of z map finitely many elements of y to an element of y. These maps artificially simulate the process of human deduction: the inputs are the antecedents (or antecedent if the inference rule is unary) and the output is the consequent.

An element $r \in z$ is an element of $[G \to y]$ for some $m \geq 1$ and $G \subseteq y^m$. This m is called the **arity** of r. We also say r is **m-ary**, **unary** if $m = 1$, and **binary** if $m = 2$.

Suppose $\beta \in y$ and $A \subseteq y$. β is a **direct consequence** of A if for some $q \leq |A|$ there is a q-ary inference rule $i \in z$ and a subset $\{a_1, ..., a_q\} \subseteq A$ such that $i\,(a_1, ..., a_q) = \beta$.

A **proof** is an element $\pi \in \bigcup_{m=1}^{\infty} [\mathbb{F}_m \to y]$ such that every $\pi\,(n)$ is either an element of some distinguished set Γ or is a direct consequence of $\pi\,[\mathbb{F}_{n-1}]$.

Definition If $\Gamma \subseteq y$ and $\psi \in y$, then $\Gamma \vdash \psi$ if and only if there exists a proof π such that $\pi\,(|\pi|) = \psi$ and every $\pi\,(n)$ is either an element of Γ or is a direct consequence of $\pi\,[\mathbb{F}_{n-1}]$. This is known as **syntactic consequence**.

Given $\Gamma \subseteq y$, the **set of theorems of Γ** is defined by

$$Con_F\,(\Gamma) := \{\psi \in y : \Gamma \vdash \psi\}\,.$$

We will drop the subscript if it is clear which formal system we are referring to.

2 Computers

Let (x, y, z) be an xyz formal system. By a **semi-ideal computer** (i.e., a **SIC**), I mean a pair of functions (C, H) with the following properties:

1. $C \in [\mathcal{P}\,(y) \times \mathbb{N}^+ \to \mathcal{P}\,(y)]$;
2. $H \in [\mathcal{P}\,(y) \times \mathbb{N}^+ \to \{0, 1\}]$;
3. $C\,(\Gamma, m) \subseteq C\,(\Gamma, m+1)$ for all Γ and m;
4. if $H\,(\Gamma, m) = 1$ then $H\,(\Gamma, m+1) = 1$; and
5. if $H\,(\Gamma, m) = 1$ then $C\,(\Gamma, m+1) = C\,(\Gamma, m)$.

Let $\|\gamma\|_\Gamma$ be the length of a shortest proof of γ from axioms Γ. Set

$$V\,(\Gamma, k) := \{\gamma \in y : \|\gamma\|_\Gamma = k\}\,.$$

Observe that we can define a SIC as follows:

$$C_1\,(\Gamma, m) := \bigcup_{k=1}^{m} V\,(\Gamma, k) = \{\gamma \in y : \|\gamma\|_\Gamma \leq m\}$$

and

$$H_1(\Gamma, m) := \begin{cases} 1 & \text{if} \quad (\forall m' \in \mathbb{N}^+)(m' \geq m \rightarrow V(\Gamma, m') = V(\Gamma, m)) \\ 0 & \text{if} \quad (\exists m' \in \mathbb{N}^+)(m' \geq m \wedge V(\Gamma, m') \neq V(\Gamma, m)) \end{cases}.$$

A SIC (C, H) is called **effective** with respect to the formal system (x, y, z) if for all $\Gamma \in \mathcal{P}(y)$, $Con(\Gamma) = \bigcup_{m=1}^{\infty} C(\Gamma, m)$. We might be more interested in **finitely effective** SICs for which there is an $m \in \mathbb{N}^+$ such that $Con(\Gamma) = \bigcup_{k=1}^{m} C(\Gamma, k)$.

An **automated theorem prover** (i.e., an **ATP**) is an effective SIC.

Note that if the generalized induction conjecture is true, to show a SIC (C, H) is an ATP it would suffice to establish two key facts: (1) $\Gamma \subseteq \bigcup_{m=1}^{\infty} C(\Gamma, m)$ and (2) $\bigcup_{m=1}^{\infty} C(\Gamma, m)$ is closed under inference rules.

Another SIC associated with a formal system is one I affectionately call Skynet. I claim that Skynet is an ATP different from the SIC I just defined.

Let $S(\Gamma, m)$ be defined for $(\Gamma, m) \in \mathcal{P}(y) \times \mathbb{N}^+$ recursively as follows: $S(\Gamma, 1) = \Gamma$. For $A \subseteq y$, let

$$Z(A) = \left\{\gamma \in y : (\exists i \in z)\left(\exists \overrightarrow{a} \in A^{air(i)}\right)(\gamma = i(\overrightarrow{a}))\right\}.$$

Let $S(\Gamma, m+1) = Z(S(\Gamma, m))$ and let $C_2(\Gamma, m) = \bigcup_{k=1}^{m} S(\Gamma, k)$. Furthermore, let

$$H_2(\Gamma, m) := \begin{cases} 1 & \text{if} \quad (\forall m' \in \mathbb{N}^+)(m' \geq m \rightarrow S(\Gamma, m') = S(\Gamma, m)) \\ 0 & \text{if} \quad (\exists m' \in \mathbb{N}^+)(m' \geq m \wedge S(\Gamma, m') \neq S(\Gamma, m)) \end{cases}.$$

Claim: (C_1, H_1) and (C_2, H_2) are different ATP's.

3 Simulations

Let (C, H) be a SIC. Letting the set of states $S = C[\mathcal{P}(y) \times \mathbb{N}^+]$, a relation $r \subseteq S^2$ is a **sim** (or **simulation)** iff for every pair of states $(p, q) \in r$ and all $m \in \mathbb{N}^+$, then there is a state q' such that $(C(p, m), q') \in r$.

Given two states p and q in S, p can be **simulated by** q, written $p \leq q$, if there is a sim r such that $(p, q) \in r$. In this case, we say q is a depth one sim of p.

Suppose $m \in \mathbb{N} \cap [2, \infty)$. q is a **depth m sim of p** iff there are m states $\{q_k \in S : k \in \mathbb{F}_m\}$ such that q_1 is a depth one sim of p, for all $k \in \mathbb{F}_{m-1}$, q_{k+1} is a depth one sim of q_k, and $q_m = q$. (To be clear, we need $|\{q_k \in S : k \in \mathbb{F}_m\}| = m$.)

Suppose that $p \leq q$ where $\{p, q\} \subseteq S$. Suppose r is a sim and q simulates p with respect to r (i.e., $(p, q) \in r$). r is **nondeterministic** iff there is a $\Gamma \in \mathcal{P}(y)$ and an $m \in \mathbb{N}^+$ such that (a) $(C(p, m), \Gamma) \in r$ and (b) $\Gamma \neq C(q, m)$. r is called **deterministic** iff it is not nondeterministic, meaning that for all $\Gamma \in \mathcal{P}(y)$ and all $m \in \mathbb{N}^+$,

$$((C(p, m), \Gamma) \in r) \rightarrow (\Gamma = C(q, m)).$$

4 Conjectures and Questions

What examples of sims are there? What examples of depth m sims are there? Does $C(C(\Gamma, m), n) = C(\Gamma, m+n)$? (No: counterexample idea. Note that when $m = n = 1$, we would have $C\left(C\left(\mathit{\Gamma},1\right),1\right)=C\left(\mathit{\Gamma},2\right)$. However, $C\left(C\left(\mathit{\Gamma},1\right),1\right)=C\left(\mathit{\Gamma},1\right)=\mathit{\Gamma}$ and so in any formal system such that $\mathit{\Gamma}\neq C\left(\mathit{\Gamma},2\right)$, $C\left(C\left(\mathit{\Gamma},1\right),1\right)\neq C\left(\mathit{\Gamma},2\right)$.)

Which of these formal systems can provide us with examples? The MIU formal system. Generalized board games like chess and tic-tac-toe. The unwinnable one-dimensional analog of tic-tac-toe with only one row of three spaces. First order logic (FOL).

Conjecture Suppose $\mathit{\Gamma}\subseteq W\subseteq Con\left(\mathit{\Gamma}\right)$ and W is closed under all inference rules in z. Then $W=Con\left(\mathit{\Gamma}\right)$. (If we let $air\left(i\right)$ denote the arity of $i\in z$, W is <u>closed under inference rules</u> in z if and only if for all $i\in z$, $i\left[W^{air(i)}\right]\subseteq W$.

Question: What is $\left|Z\left(A\right)\right|$ in relation to $\left|A\right|$?