JAM CHEATSHEET

0.1. **TODO.**

- E_T**:** TODO

0.2. **State.**

- σ**:** State Identifier
- Υ**:** State Transition Function (STF)

0.3. **Misc.**

- $y \prec x$**:** precedes operator, relation to indicate one term may be defined purely in terms of another
- $\mathcal{U}$**:** substitute-if-nothing function
- i, j**:** used for numerical indices
- $\varnothing$**:** nothing

0.4. **Functions and Operations.**

- $\exists$**:** exists
- $\Longleftrightarrow$**:** TODO (section 3.2)
- $\bigwedge_{i=0}^{x-1}$**:** big wedge

0.5. **Sets.**

- x, y**:** item of a set or sequence
- $\mathbf{s}$**:** set
- $\wp\langle\mathbf{s}\rangle$**:** set power (section 3.3)
- $|\mathbf{s}|$**:** set cardinality (section 3.3)
- $f^{\#}$**:** function applied to all members of a set to yield a new set (section 3.3)
- $⫰$**:** set-disjointness relation (section 3.3)
- ∇**:** indicates unexpected failure of an operation or that a value is invalid or unexpected (section 3.3)

0.6. **Numbers.**

- $\mathbb{N}$**:** denotes the set of naturals including zero
- $\mathbb{N}_n$**:** restricts the set of naturals to values less than n.
  - Formally, $\mathbb{N} = \{0, 1, \dots\}$ and $\mathbb{N}_n = \{x \mid x \in \mathbb{N}, x < n\}$
- $\mathbb{N}_L$**:** is equivalent to $\mathbb{N}_{2^{32}}$ and denotes the set of lengths of octet sequences that must have limited size to be stored practically
- $\%$ **:** modulo operator
- $5 \div 3 = 1 \,\mathsf{R}\, 2$**:** remainder of quotient operation

0.7. **Integers.**

- $\mathbb{Z}$**:** denotes the set of integers
- $\mathbb{Z}_{a\dots b}$**:** denotes the set of integers within the interval $[a, b)$
  - Formally, $\mathbb{Z}_{a\dots b} = \{x \mid x \in \mathbb{Z}, a \le x < b\}$ (e.g. $\mathbb{Z}_{2\dots 5} = \{2, 3, 4\}$).
  - $\mathbb{Z}_{a\cdots+b}$ denotes the offset/length form of this set, which is a short form of $\mathbb{Z}_{a\dots a+b}$.

0.8. **Dictionaries.**

- $\mathbb{D}\langle \mathrm{K} \to \mathrm{V}\rangle$**:** denotes a dictionary mapping from domain K to range V
- $\mathbb{D}$**:** set of all dictionaries
- $(k \mapsto v)$**:** key-value pair in dictionary
- $\mathbb{D} \subset \left\{\{(k \mapsto v)\}\right\}$**:** defines a dictionary as a member of the set of all dictionaries $\mathbb{D}$ and a set of pairs $p = (k \mapsto v)$
- $\forall \mathbf{d} \in \mathbb{D} : \forall (k \mapsto v) \in \mathbf{d} : \exists! v' : (k \mapsto v') \in \mathbf{d}$**:** dictionary's members must associate at most one unique value for any key k
- $\forall \mathbf{d} \in \mathbb{D} : \mathbf{d}[k : \equiv \begin{cases} v & \text{if } \exists k : (k \mapsto v) \in \mathbf{d} \\ \varnothing & \text{otherwise} \end{cases}]$ define the subscript operator for a dictionary d
  - Note, assumes the key exists in the dictionary, otherwise the result is undefined and any block relying on it must be considered invalid
- $\forall \mathbf{d} \in \mathbb{D}, \mathbf{s} \subseteq K : \mathbf{d} \setminus \mathbf{s} \equiv \{(k \mapsto v) : (k \mapsto v) \in \mathbf{d}, k \notin \mathbf{s}\}$**:** define the subtraction operator for a dictionary d
- $\mathbb{D}\langle K \to V\rangle \subset \mathbb{D}, \mathbb{D}\langle K \to V\rangle \equiv \left\{\{(k \mapsto v) \mid k \in K \wedge v \in V\}\right\}$ **:** denotes a typed dictionary mapping from domain K to range V as a set of pairs p of the form $(k \mapsto v)$
- $\mathcal{K}(\mathbf{d} \in \mathbb{D}) \equiv \{\ k \mid \exists v : (k \mapsto v) \in \mathbf{d}\ \}, \mathcal{V}(\mathbf{d} \in \mathbb{D}) \equiv \{\ v \mid \exists k : (k \mapsto v) \in \mathbf{d}\ \}$**:** denotes the active domain (i.e. set of keys) of a dictionary $\mathbf{d} \in \mathbb{D}\langle K \to V\rangle$, using $\mathcal{K}(\mathbf{d}) \subseteq K$, and range (i.e. set of values) $\mathcal{V}(\mathbf{d}) \subseteq V$, where since the co-domain of $\mathcal{V}$ is a set, if different keys with equal values appear in the dictionary, the set will only contain one such value.
- $\forall \mathbf{d} \in \mathbb{D}, \mathbf{e} \in \mathbb{D} : \mathbf{d} \cup \mathbf{e} \equiv (\mathbf{d} \setminus \mathcal{K}(\mathbf{e})) \cup \mathbf{e}$**:** dictionaries combined through the union operator $\cup$, which prioritizes the right-side operand in the case of a key-collision.
- $\mathcal{K}(\mathbf{d})$**:** returns active domain (set of keys) of dictionary
- $\mathcal{V}(\mathbf{d})$**:** returns range (set of values) of dictionary

0.9. **Tuples.**

About: Tuples are groups of values where each item may belong to a different set

- (a, b)**:** tuple notation
- $(\mathbb{N}, \mathbb{N})$**:** set of natural pairs
- $\mathbf{T} = (a \in \mathbb{N},\ b \in \mathbb{N})$**:** tuple with named components
- t_a, t_b**:** access named components of tuple
- **:** e.g. denote an item $t \in T$ through subscripting its name, so for some $t = (a\colon 3,\ b\colon 5)$, $t_a = 3$ and $t_b = 5$

0.10. **Sequences.**

- $[\![T]\!]$**:** set of sequences with elements from set T, and defines a partial mapping $\mathbb{N} \to T$
- $[\![T]\!]_n$**:** set of sequences with exactly n elements from set T, and defines a complete mapping $\mathbb{N}_n \to T$
- $[\![T]\!]_{:n}$**:** set of sequences with at most n elements
- $[\![T]\!]_{n:}$**:** set of sequences with at least n elements
- $\mathbf{s}_i$**:** access item at index i in sequence $\mathbf{s}$
- $[0, 1, 2, 3 : \ _{\dots 2} = [0, 1]$ and $[0, 1, 2, 3]_{1\cdots+2} = [1, 2]]$ range in a sequence
- $|\mathbf{s}|$**:** length of sequence
- $\mathbf{s}[i : \ ^{\circlearrowleft} \equiv \mathbf{s}[\ i \ \%\ |\mathbf{s}|\ ]]$ modulo subscription
- $\mathbf{last}(\mathbf{s}) \equiv x$**:** function that returns final element x of a sequence $\mathbf{s} = [..., x]$
- $\frown$**:** sequence concatenation operator
- $\hat{\mathbf{x}}$**:** concatenate-all operator for sequences of sequences
- $x +\!\!\!+\, i$**:** element concatenation

0.11. **Cryptography.**

- $\mathbb{H}$**:** set of 256-bit values from cryptographic functions (equivalent to $\mathbb{Y}_{32}$)
- $\mathbb{H}^0$**:** equals $[0]_{32}$
- $\mathcal{H}(m)$**:** Blake2b 256-bit hash function
- $\mathcal{H}_K(m)$**:** Keccak 256-bit hash function
- $\mathcal{H}_x(m)$**:** first x octets of hash

0.12. **Boolean & Octets.**

- $\mathbb{B}_s$**:** set of Boolean strings of length s
- $\mathbb{Y}$**:** set of octet strings ("blobs") of arbitrary length
- $\mathbb{Y}_x$**:** set of octet strings of length x
- $\mathbb{Y}_\$$**:** subset of $\mathbb{Y}$ which are ASCII-encoded strings
- **bits**($\mathbb{Y}$)**:** sequence of bits representing octet sequence