An Approach to Developing on Urbit

N E Davis

April 15, 2021

Malancandra & Sons

Colophon
This document was typeset with the help of KOMA-Script and LaTeX using the kaobook class.
The source code of this book is available at:
https://github.com/davis68/urbit-textbook

Publisher
First printed in July 2022 by Malancandra & Sons

Lights All Askew in the Heavens.
Stars Not Where They Seemed or Were Calculated to Be.
A BOOK FOR 12 WISE MEN.
No More in All the World Could Comprehend It.

– *The New York Times*, November 19, 1919

Contents

List of Figures

List of Tables

A Brief Introduction 1

1.1 What We Talk About When We Talk About Urbit

Urbit is a functional-as-in-language, network-first, compatibility-breaking operation function (or hosted operating system). But what does any of this mean? As we explore Urbit software development throughout this book, keep in mind that every piece of Urbit aims to solve a ambitious battery of critical problems with the existing legacy World Wide Web.

A Series of Unfortunate Events

Centralization . For most contemporary corporations, whether enterprise-scale or startup, the driving factor for growth and revenue became the number of customers (users) they were able to attract to their platform or app. Services like `del.icio.us` (founded 2003) and Flickr (founded 2004) betokened a wave of massive centralization, cemented by Facebook, Google, and Apple in the late aughts. TODO XXX number of users on each in 2010

As users jostled onto burgeoning social media platforms, their patterns of behavior changed, and more and more social interactions of significance took place within "walled gardens," service platforms that interfaced only poorly with the exterior web. Vendor lock-in and the nonportability of user data between platforms meant that consumer choice became a byword. It became (and remains) difficult for any user to find out just what a corporation or even an app knows about them, particularly given the rise of surveilling cookies and data trackers.

The shift to mobile computing starting with the 2007 launch of Apple's iPhone drove a rise in cloud computing and cloud storage. To many users, the data storage and access permissions on their data became largely illegible. Sometimes this led to poor assumptions, such as that the custodial corporation would never allow a leak, or that the data would always be backed up safely. As projects failed (like `del.icio.us`) or unilaterally changed policies (Tumblr), users permanently lost data. Given the effort involved in curating tags, bookmarks, images, contacts, and research data, these outcomes frequently amounted in the loss of years of human effort.

Data leaks . During the 2000s and 2010s, data leaks became so common as to hardly merit notice. As users flocked to corporate platforms for social media, publishing, photography, dating, and every other aspect of digital life, insufficient attention was given by corporations to both the practical security of user data and the potential fallout of leaks. Data

breaches grew in number ever year, and affected corporations of every size in every industry.

- 2013: Evernote, 50 million records
- 2014: Ebay, 145 million records
- 2015: Ashley Madison, 32 million records
- 2016: Yahoo!, 1 billion records
- 2017: Experian, 147 million records
- 2019: Facebook, 850 million records
- 2019: CapitalOne, 106 million records

("Records" does not equal "people" or even "accounts," of course, rendering these numbers mutually incommensurable. Regardless, the scale staggers the mind.) Sometimes these breaches were the result of clever social engineering; more frequently, someone forgot to properly salt password hashes or just stored or transmitted them in unencrypted plaintext. Occasionally, the data were even just left available at a deprecated or forgotten API endpoint. Identity security is challenging to get right, and those who had custody of user data were frequently subject to moral hazard.

The looming software stack . A combination of practical manufacturing limits ending Moore's law and a complexifying operating system and software stack led to a long-term stagnation in the perceived speed and fluidity of user experience with computers. For the most part, even as multicore CPUs become more widespread, software bloat grows more acute with each new operating system version. For many enterprise developers, there have been insufficient incentives to simplify software rather than to continue making it more complex. Minimalist software by and large remained the demesne of hackers and code golf enthusiasts.

For instance, TODO MS Word menu structure and file bloat

Even websites with visually minimalist aesthetics often presented **Ceglowski2015** a - Optional Reading: Maciej Cegłowski, "The Website Obesity Crisis"

- Optional Reading: Maciej Cegłowski, "Build a Better Monster: Morality, Machine Learning, and Mass Surveillance"

- Optional Reading: Mark Tarver, "The Cathedral and the Bizarre"

Security breaches . As the softwar stack grows, dependencies become opaque to downstream developers and users. Upstream vulnerabilities have led to zero-day exploits and security breaches. For instance, in 2014 the popular OpenSSL cryptography package had a bug of two years' standing revealed, Heartbleed. This flaw in the Transport Layer Security (TLS) exposed memory buffers adjacent to

Instant-messaging protocols relying on the `libpurple` were impacted by an out-of-bounds write flaw in 2017, potentially permitting denial-of-service attacks or arbitrary code execution.

These two examples are not cherry-picked: other examples abound. The point stands that security breaches in the software stack render reliant software vulnerable in unpredictable ways.

Morbidity in open-source software projects . The rise of the free and open-source software (FOSS) movement has been enormously influential on software development and the end-user experience. Spearheaded by Richard Stallman's GNU Project and Linus Torvalds' Linux operating system, FOSS rapidly overtook enterprise software offerings in terms of feature parity and upstream utilization.

Unfortunately, open-source software products are frequently broken in ways that are opaque to relatively nontechnical users:

1. FOSS can be construed as operating under a parasitic model. Most real innovation happens outside of open-source projects, which are often clones of more successful proprietary software packages (LibreOffice/Microsoft Office, GIMP/Adobe Photoshop, Inkscape/Adobe Illustrator), and/or a clever way for a company to farm out development to free community labor (OpenOffice/Oracle, Ubuntu/Canonical, Darwin/Apple). Thus even FOSS successes are often copies of proprietary antecedents.
2. FOSS suffers from [what one observer has dubbed](http://marktarver.com/thecathedralandthebizarre.html) "financial deficiency disease." Even popular, well-used packages may have little oversight and funding for developers. As alluded to above, OpenSSL was found in 2014 to have only one full-time developer despite being used by 66% of Internet users. Very few companies have succeeded in being FOSS-first (as opposed to FOSS-sometimes).
3. FOSS has a hard time responding to customer demands. The DIY ethos espoused by FOSS developers has often led to demurrage when features are requested. This is the infamous response, "If you need it, why don't you build it yourself?" Many users are unable to commit the time to implement the necessary features, and most FOSS projects do not have full-time developers and existing market dynamics sufficient to motivate rapid development.

Even companies that loudly proclaimed support for "data liberation" used this FOSS openness like a lanternfish to later replace an open protocol (*e.g.*, Google Talk) with a proprietary one (Google Hangouts).

Given the cascading stack of legacy software and strange interdependencies, actually getting the secure functionality a user wants often requires a proprietary platform anyway, undermining the aims of FOSS end-user applications and libraries.

Identity is cheap . Identity itself is cheap: it costs botnets and spammers nothing to spin up new email addresses and new false identities. Game-theoretically, spammers thrive in an environment where identity is close to free.

Identity is also dear: losing a password in a breach can cause at best hours of resetting service logins and at worst the trauma and legal process of recovering from identity theft.

The foregoing summation may read as a bit emotional relative to what the reader is accustomed to reading in an academic textbook. This is because the structure of our digital life matters as much as the content, and we have been ill-served to date by the incentives and powers that be.

Enter Urbit, stage right.

Why Urbit

"Urbit is a clean slate reimagining of the operating system as an 'overlay OS', and a decentralized digital identity system including username, network address and crypto wallet." (Tlon)

The Urbit project intends to cut the Gordian knot of user autonomy and privacy. To this end, the Urbit developers have articulated an approach prioritizing *a legible future-proof program stack*, *data security*, and *cryptographic ownership*. The ambitious scope of this project—and the evolution of the goals over the decade of the 2010s—has led many to have difficulty grasping what exactly Urbit is all about. Urbit has been built to provide an Internet where communities can thrive without meddling or interference by third parties, and where what you build truly belongs to you.

"[Urbit is] ultimately a hosted OS ([residing] on top of Linux) with an immutable file system with the additional purpose that you build applications distributed-first in a manner where clients store their own data." (['scare-junba'](https://news.ycombinator.com/item?id=21672481))

Your Urbit is a personal server built as a functional-as-in-language operating system that runs as a virtual machine on top of whatever. (Sometimes the developers refer to this arrangement as a "hosted OS," but they don't mean as in VMWare or VirtualBox or even containerization.) The Urbit vision is the unification of services and data around a scarce futureproof identity on an innately secure platform. Briefly put, Urbit requires you to have an *Urbit OS* (which runs your code, stores your data, etc.) and an *Urbit ID* (which secures your ownership of said code and data).

Urbit provides an excellent example of a visionary complex system which is radical (returning to the roots of computing) and forward-looking—and yet still small enough for us to grok all of the major moving parts in the system. As a "hundred-year computer," Urbit represents how computing could work when computing power approaches negligible cost and bandwidth becomes effectively unlimited (or at least not limiting), instead focusing on the quality of user experience and user security. We have found that Urbit is worthy of study in its own right as a compelling clean-state architecture embracing several innovative ideas at its base.

Legible future-proof program stack . The core of Urbit is an *operating function*, or a functional-as-in-language operating system. That is, there is a lifecycle function which receives a state and an event, processes the event, and yields a new state.

$$L(\sigma, \varepsilon) \to \sigma'.$$

This is called the Urbit OS to distinguish it from other aspects of the Urbit project when ambiguity is present. The Urbit OS lifecycle function is written in a language called Nock and provides operational affordances through the Arvo operating core. A schematic representation is frequently used:

: width=25

At its base, Arvo is an encrypted event log yielding a particular state. The Nock virtual machine is like Urbit's version of assembler language, and it may in principle be implemented on top of any hardware. Hoon is Urbit's equivalent of C, a higher-level language with useful macros and APIs for building out software. Arvo runs atop these definitions.

The user can think of Urbit OS as a virtual machine which allows everything upstack to be agnostic to the hardware, and handles everything downstack. Urbit has sometimes been described as an operating function, and this is what that means. Everything is implemented as a stateful instance, called a "ship."

: width=50

The vanes of Arvo provide services: `%ames` provides network interactivity, `%clay` provides filesystem services and builds, `%jael` provides cryptographic operations, and so forth. On top of these are built the userspace apps.

We will take a closer look at every part of this system in Chapter **??**.

: width=100

As a "hosted OS," Urbit doesn't seek to replace mainline operating systems. Indeed, presumptively its Nock virtual machine could be run quite close to the bare metal, but Urbit itself would still require some provision of memory management, hardware drivers, and input/output services. The overarching goal of the Urbit project is instead to replace the insecure messaging and service platforms and protocols used across the current web.

Urbit was designed on the principle that inheriting old platform code is a developer antipattern, given the complexities, vagaries, and vulnerabilities of legacy OSs. In other words, things must break to be fixed. Thus Urbit interfaces with other systems, but is a world unto itself internally.

Data security . TODO

Cryptographic ownership . We noted above that Urbit OS is an encrypted event log. Urbit also acts as a universal single sign-on (SSO) for the platform and for services instrumented to work with Urbit calls. Since the Urbit address space is finite, each Urbit ID has inherent value within the system and should be a closely guarded secret. An instantiation of your Urbit ID is frequently called a *ship*, which lodges on your filesystem at a folder called a *pier*.

Following in the footsteps of other blockchain technologies, Urbit secures ownership of unique access points in the Urbit address space using Azimuth. Currently Azimuth is deployed on top of the Ethereum blockchain.

See Section **??** for more details.

Urbit IDs have mnemonic names attached to them, although fundamentally they are only a number in the address space. For instance, one example address on Urbit is `dopzod-binfyr`, the unique ID one user owns, corresponding to the 32-bit address `0xeb2a.5a32` in hexadecimal.

On this network-oriented platform, users provide data to service endpoints, retaining their data rather than farming it out. While no control can be exercised over data once sent out, a proposed reputation system can penalize bad actors in the system with reduced network access and other sanctions.

Let us posit a social operating system, or SOS; a protocol for network-oriented platforms to utilize to ensure that user requirements are met

securely. If we enumerate user-oriented desiderata for a social operating system, surely the following must rank prominently:

TODO

Thompson1984

The system is designed to be transparent. Something that runs on the Nock VM is of necessity open-source—no binary blobs! (As with Ken Thompson's "Reflections on Trusting Trust", one can't necessarily trust what's below completely, but that's a problem with any system one did not build oneself from the bare metal up.)

Identity on the current Web is frequently ephemeral and difficult to distinguish from spam. Identity on Urbit is scarce and stable, much like moving into a house. The SSO aspect of the system means that you have to remember and use many fewer passwords, and the cryptographic security layers means that as long as you treat your master key like your Bitcoin wallet you will have perpetual security.

At this point, you may feel confused as to what exactly Urbit is. That's understandable: it's hard to explain a new system in full until it has started to manifest new and interesting features with broader repercussions. For comparison, consider the following two interviews from much earlier in the history of the public Internet:

- Bill Gates on David Letterman, 1995 (an attempt to explain the Internet before almost anyone grokked it)
- David Bowie on the BBC, 1999 (a prophecy which grasps the essence without the technicality)

On this basis, it's safe to say that Gates got it, but Bowie "got it." Their interlocutors did not.

The Urbit project does not completely solve all of these problems—for instance, pwned hardware—but it offers a reasonable set of solutions for many of the social and software issues raised by contemporary corporate practice on the World Wide Web. Many think that it is better to attempt to fix the challenges of data control, privacy, and equity on the current web: Sovrin, WebAssembly, InterPlanetary File System, Holochain, Space, and Scuttlebutt each, in their own way, attack the same problems that Urbit seeks to solve, and each is worthy of the reader's further study.

All in all, Urbit like Bitcoin and (the best) blockchain applications seeks to securely deliver on the aims of the old Cypherpunk movement of the 1980s and 1990s: digital security, digital autonomy.

1.2 Azimuth, the Urbit Address Space

In **Zooko2001**, digital cash pioneer Zooko Wilcox-O'Hearn postulated that a namespace cannot simultaneously possess three qualities:

1. distributedness ("in the sense that there is no central authority which can control the namespace, which is the same as saying that the namespace spans trust boundaries"),
2. security ("in the sense that name lookups cannot be forced to return incorrect values by an attacker, where the definition of "incorrect" is determined by some universal policy of name ownership"), and
3. human legibility (or interpretable by human users).

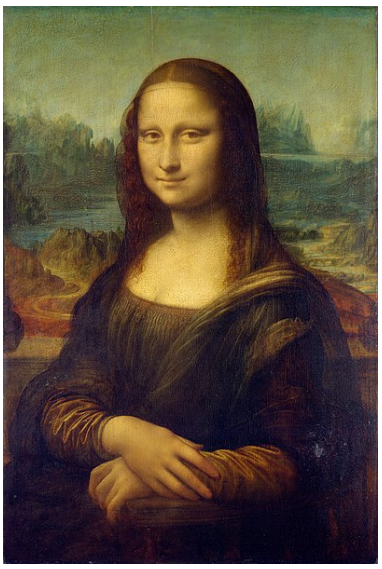

Figure 1.1: Some sigils
`https://media.urbit.org/site/posts/essays/help-the-environment.jpg`

This trilemma, dubbed Zooko's triangle, laid down a challenge to cryptographic researchers, who spent some effort to empirically refute the postulate.

In the case of Urbit,

1.3 A Frozen Operating System

The philosophy underlying Urbit bears a strange resemblance to mathematics: rather than running always as fast as one can to stay in the same place (a Red Queen's race), one should instead establish a firm foundation on which to erect all future enterprises. In this view, the operating system should provide a permanently future-proof platform for launching your applications and storing your data—rather than a pastiche of hardware platforms and network specifications, all of that is hidden, "driver-like." The OS should explicitly obscure all of that and no reaching beneath the OS should be allowed.

From [the docs](https://web.archive.org/web/20140424223249/http://urbit.org/community/articles/martian-computing/):

> Normally, when normal people release normal software, they count by fractions, and they count up. Thus, they can keep extending and revising their systems incrementally. This is generally considered a good thing. It generally is.
>
> In some cases, however, specifications needs to be permanently frozen. This requirement is generally found in the context of standards. Some standards are extensible or versionable, but some are not. ASCII, for instance, is perma-frozen. So is IPv4 (its relationship to IPv6 is little more than nominal - if they were really the same protocol, they'd have the same ethertype). Moreover, many standards render themselves incompatible in practice through excessive enthusiasm for extensibility. They may not be perma-frozen, but they probably should be.
>
> The true, Martian way to perma-freeze a system is what I call Kelvin versioning. In Kelvin versioning, releases count down by integer degrees Kelvin. At absolute zero, the system can no longer be changed. At 1K, one more modification is possible. And so on.

Urbit (currently) refers to this way of doing things as "Martian."

In other words, Urbit is intended to cool towards absolute zero, at which point its specification is locked in forever and no further changes are countenanced. This doesn't apply to everything in the system—"there simply isn't that much that needs to be versioned with a kelvin" (nidsut-tomdun)—but it does apply to the most core components in the system.

Urbit is not, of course, the only system to adopt an asymptotic approach to its final outcome. Donald Knuth, famous for many reasons but in this particular instance for the typesetting system TEX, has specified that TEX versions incrementally approach π. TEX will reach π definitively upon the date of Knuth's death, at which point all remaining bugs are instantly transformed into features and the version becomes π. The current version of TeX is 3.14159265.

In this light, when we talk about Urbit we talk about three things:

1. Crystalline Urbit (the promised frozen core, 0K)
2. Fluid Urbit (the practice, mercurial and turbulent but starting to take shape)
3. Mechanical Urbit (the under-the-hood elements, still a chaos lurching into being, although much less primeval than before)

Think of the hypothetical structure of Jupiter: clouds over a sea of metallic hydrogen over a diamond as big as Earth. TODO image.

1.4 Developing for Urbit

The primary aim of this textbook is to expound Urbit in sufficient depth that you can approach it as an effective software developer. We assume

previous programming experience of one kind or another, not necessarily in a functional language.

Urbit development can be divided into three cases:

1. Kernel development
2. Userspace development, Urbit-side (`%gall` and generators)
3. Userspace development, client-side (Urbit API)

dojo ships fakezods

This guide focuses on getting the reader up to speed on the second development case early, then branches out into the two others. With a solid foundation in `%gall`, the reader will be well-equipped to handle demands in either of the other domains. We encourage the reader to approach each example and exercise in the following spirit:

1. Identify the input and outputs, preferably at the data type level and contents.
2. Reason analogically from other Hoon examples available in the text and elsewhere.
3. Create and complete an outline of the code content.
4. Devise and compose a suitable test suite.

1.5 Exercises

1. Obtain an Urbit ID and set up your Urbit OS. Use the current installation procedure outlined at `urbit.org`. You do not need to use a hosting service if you prefer to run Urbit on your own hardware, but maintaining your ship in an always-connected state will improve your experience.
2. Set up a fakezod for software development.

Language Essentials

Nock, A Combinator Language

2

2.1 Primitive rules and the combinator calculus

A combinator calculus is one way of writing primitive computational systems. Combinatory logic allows one to eliminate the need for variables (unknown quantities like x) and thus deal exclusively (?) with pure functions.

one combinator calculus

To understand how Nock expressions produce nouns as pure stateless functions, we need to introduce the *subject*. The subject is somewhat analogous to a namespace in other programming languages; it encompasses the computational context and the arguments. Another way to put it is that the subject *is* the argument to the Nock formula: not all of the subject may be used in evaluating the formula, but it is all present.

Nock is a crash-only language; that is, while it can emit events that are interpretable by the runtime as errors that can be handled, Nock itself fails when an invalid operation occurs.

Nock is a standard of behavior, not necessarily an actual machine. (It is an actual machine, of course, as a fallback, but the point is that any Nock virtual machine should implement the same behavior.) We like to think of this analogous to solving a matrix. Formally, given an equation

$$A\vec{x} = \vec{b}$$

the solution should be obtained as

$$A^{-1}A\vec{x} = A^{-1}\vec{b} \rightarrow \vec{x} = A^{-1}\vec{b}$$

This is correct, but often computationally inefficient to achieve. Therefore we use this behavior as a standard definition for $\vec{x}$, but may actually obtain $\vec{x}$ using other more efficient methods. Keep this in mind with Nock: one has to know the specification but doesn't have to follow suit to implement it this way (thus, jet-accelerated Nock, Section **??**).

Nock 4K

The current version of Nock, Nock 4K, consists of six primitive rules as well as a handful of compound adjuncts. The primitive rules are conventionally written in an explanatory pseudocode:

`*[a 0 b]`	`/[b a]`
`*[a 1 b]`	`b`
`*[a 2 b c]`	`*[*[a b] *[a c]]`
`*[a 3 b]`	`?*[a b]`
`*[a 4 b]`	`+*[a b]`
`*[a 5 b c]`	`=[*[a b] *[a c]]`

with the following operations:

- $*$ is the *evaluate* operator, which operates on a cell of `[subject formula]`;
- `/` is the *slot* operator or address `b` of [tree] `a`;
- `?` is the *cell* operator, testing whether its operand is a cell.
- `+` is the *increment* operator.
- `=` is the *equality* operator, checking for structural equality of the operands evaluated against the subject `a`.

It is also instructive to write these as mathematical rules:

$$
\begin{aligned}
*_0[a](b) &:= a_b \\
*_1[a](b) &:= b \\
*_2[a](b,c) &:= *(*[a](b), *[a](c)) \\
*_3[a](b) &:= \begin{cases} \text{true} & \text{if cell} \\ \text{false} & \text{if atom} \end{cases} \\
*_4[a](b) &:= *(a,b) + 1 \\
_5[a](b,c) &:= ((a,b) \stackrel{?}{=} *(a,c))
\end{aligned}
$$

where $*$ is the generic evaluate operator. Furthermore, true is the integer 0 while false is the integer 1. Each rule is referred to by its number; *e.g.*, "Nock 3" refers to the cell test rule.

Nock operates on unsigned integers, with zero 0 expressing the null or empty value. Frequently this is written as a tilde, ~ or ~. This value plays a complex role similar to `NULL` and `'\0'` in C and other programming languages—although, critically, it is still numeric.

Nock 0, Addressing

`*[a 0 b]`	`/[b a]`

$$*_0(a,b) := a_b$$

Nock Zero allows the retrieval of nouns against the Nock subject. Data access requires knowing the address and how to retrieve the corresponding value at that address. The slot operator expresses this relationship using `a` as the subject and the atom `b` as the one-indexed address.

Every structure in Nock is a binary tree. Elements are enumerated left-to-right starting at 1 for the entire tree.

One common convention is to store values at the leftward leaves of rightward branches; this produces a cascade of values at addresses $2^n - 2$.

The address of a value in the Nock binary tree has no direct correspondence to its address in physical memory. This latter is handled by the Nock runtime, avoiding the use of pointers in Nock code.

By hand,

In the Dojo, you may evaluate this statement using the `.*` "dottar" rune:

```
.*(TODO)
```

You may also use `++mock`

virtualization arm computes a formula. '++mock' is Nock in Nock, however, so it is not very fast or efficient.

'++mock' returns a tagged cell, which indicates the kinds of things that can go awry:

- '-
- '-
- '

'++mock' is used in Gall and Hoon to virtualize Nock calculations and intercept scrys. It is also used in Aqua, the testnet infrastructure of virtual ships.

Nock 1, Constant Reduction

```
*[a 1 b]            b
```

$$*_1(a, b) := b$$

Nock One simply returns the constant value of noun `b`.

Nock 2, Evaluate

```
*[a 2 b c]          *[*[a b] *[a c]]
```

$$*_2[a](b, c) := *(*[a](b), *[a](c))$$

Nock 3, Test Cell

Although unusual, Nock is by no means the only language to adopt 0 as the standard of truth. The POSIX-compliant shells such as Bash adopt the convention that 0 is `TRUE`. So do Ruby and Scheme, although with caveats.

Nock Three zero as true (because there is one way to be right and many ways to be wrong). loobean

Nock 4, Increment

Nock 5, Test Equivalence

Let us examine some Nock samples by hand and see if we can reconstruct what they do. We will then create some new short programs and apply them by hand via the Nock rules.

2.2 Compound rules

For the convenience of programmers working directly with Nock (largely the implementers of Hoon), a number of compound rules were defined that reduce to the primitive rules. These implement slightly higher-order conventions such as a decision operator. Each of these provide syntactic sugar that render Nock manipulations slightly less cumbersome.

```
*[a 6 b c d]          *[a *[[c d] 0 *[[2 3] 0 *[a 4 4 b]]]]
*[a 7 b c]            *[*[a b] c]
*[a 8 b c]            *[[*[a b] a] c]
*[a 9 b c]            *[*[a c] 2 [0 1] 0 b]
*[a 10 [b c] d]       #[b *[a c] *[a d]]

*[a 11 [b c] d]       *[[*[a c] *[a d]] 0 3]
*[a 11 b c]           *[a c]
```

with the following operation:

- `#` is the *replace* operator, which edits a noun by replacing part of it with another piece.

As mathematical rules, these would be:

$$
\begin{aligned}
*_6[a](b,c,d) &:= \begin{cases} *[a](c) & \text{if } b \\ *[a](d) & \text{otherwise} \end{cases} \\
*_7[a](b,c) &:= *[*[a](b)](c) \\
*_8[a](b,c) &:= *[*[*[a](b)](a)](c) \\
*_9[a](b,c) &:= \begin{cases} 0 & \text{if cell} \\ 1 & \text{if atom} \end{cases} \\
*_{10}[a](b,c,d) &:= *(a,b) + 1 \\
_{11}[a](b,c,d) &:= ((a,b) \stackrel{?}{=} *(a,c)) \\
_{11}[a](b,c) &:= ((a,b) \stackrel{?}{=} *(a,c))
\end{aligned}
$$

where $*$ is the generic evaluate operator.

Nock 6, Conditional Branch

Nock 7, Compose

Nock 8, Declare Variable

Nock 9, Produce Arm of Core

Nock 10, Replace

Nock 11, Hint to Interpreter

With Nock under your belt, many of the quirks of Hoon become more legible. For instance, since everything in Nock is a binary tree, so also

There's also a "fake Nock" Rule Twelve, `.^` "dotket", which exposes a namespace into Arvo. More details on this follow in Section **??**.

everything in Hoon. Nock also naturally gives rise to cores, which are a way of pairing operations and data in a cell.

Although Nock is the runtime language of Urbit, developers write actual code using Hoon. Given a Hoon expression, you can produce the equivalent Nock formula using `!=` "zaptis".

After this chapter, you may never write Nock code again. That's fine! We need to understand Nock to understand Hoon, but will not need to compose in Nock directly to do any work in Urbit, even low-level work. (There is no `inline` equivalent.)

```
> !=(+(1))
[4 1 1]

> !=((add 1 1))
[8 [9 36 0 1.023] 9 2 10 [6 [7 [0 3] 1 1] 7 [0 3] 1 1] 0 2]
```

(Why do these differ so much? `++add` is doing a bit more than just adding a raw 1 to an unsigned integer. We'll walk through this function later in Section TODO.)

One last piece is necessary for us to effectively interpret Nock code: the implicit cons. Cons is a Lisp function to construct a pair, or what in Nock terms we call a cell. Many times we find Nock expressions in which the operand is a cell, and so TODO

Nock Examples

We will work through several Nock programs by hand. Since each Nock program is a pure function and emits no side effects, when we have applied all of the rules to achieve a final value, we are done calculating the expression.

Infamously, Nock does not have a native decrement operator, only an increment (Rule Four). Let us dissect a simple decrement operation in Nock:

```
> !=(|=(a=@ =+(b=0 |-(?:(=(a +(b)) b $(b +(b)))))))
[ 8
  [1 0]
  [1 8 [1 0] 8 [1 6 [5 [0 30] 4 0 6] [0 6] 9 2 10 [6 4 0 6] 0
    1] 9 2 0 1]
  0
  1
]
```

which can be restated in one line as

```
[8 [[1 0] [1 8 [1 0] 8 [1 6 [5 [0 30] 4 0 6] [0 6] 9 2 10 [6 4
     0 6] 0 1] 9 2 0 1] 0 1]]
```

or in many lines as

```
[8
  [1 0]
  [1 [8
       [1 0]
```

```
        [8
          [1 [6
                [5
                  [0 30]
                  [4 0 6]
                ]
                [0 6]
                [9
                  2
                  [10
                    [6 4 0 6]
                    [0 1]
                  ]
                ]
              ]
            [9 2 0 1]
          ]
        ]
      ]
    ]
    [0 1]
]
```

(It's advantageous to see both.)

We can pattern-match a bit to figure out what the pieces of the Nock are supposed to be in higher-level Hoon. From the Hoon, we can expect to see a few kinds of structures: a trap, a test, a 'sample'. At a glance, we seem to see Rules One, Five, Six, Eight, and Nine being used. Let's dig in.

(Do you see all those '0 6' pieces? Rule Zero means to grab a value from an address, and what's at address '6'? The 'sample', we'll need that frequently.)

The outermost rule is Rule Eight '*[a 8 b c]→*[[*[a b] a] c]' computed against an unknown subject (because this is a gate). It has two children, the 'b' '[0 1]' and the 'c' which is much longer. Rule Eight is a sugar formula which essentially says, run '*[a b]' and then make that the head of a new subject, then compute 'c' against that new subject. '[0 1]' grabs the first argument of the 'sample' in the 'payload', which is represented in Hoon by 'a=@'.

The main formula is then the body of the gate. It's another Rule Eight, this time to calculate the 'b=0' line of the Hoon.

There's a Rule One, or constant reduction to return the bare value resulting from the formula.

Then one more Rule Eight (the last one!). This one creates the default subject for the trap `$`; this is implicit in Hoon.

Next, a Rule Six. This is an 'if'/'then'/'else' clause, so we expect a test and two branches.

- The test is calculated with Rule Five, an equality test between the address '30' of the subject and the increment of the 'sample'. In Hoon, '=(a +(b))'.

- The `[0 6]` returns the 'sample' address.

- The other branch is a Rule Nine reboot of the subject via Rule Ten. Note the '[4 0 6]' increment of the 'sample'.

Finally, Rule Nine is invoked with '[9 2 0 1]', which grabs a particular arm of the subject and executes it.

Contrast the built-in '++dec' arm:

```
> !=((dec 1))
[8 [9 2.398 0 1.023] 9 2 10 [6 7 [0 3] 1 1] 0 2]
```

for which the Hoon is:

```
++  dec
  |=  a=@
  ?<  =(0 a)
  =+  b=0
  |-  ^-  @
  ?:  =(a +(b))  b
  $(b +(b))
```

Scan for pieces you recognize: the beginning of a cell is frequently the rule being applied.

In tall form,

```
[8
  [9
    [2.398 [0 1.023]]
  ]
  [9 2
       [10
         [6 7 [0 3] 1 1]
         [0 2]
       ]
  ]
]
```

What's going on with the above `++dec` is that the Arvo-shaped subject is being addressed into at '2.398', then some internal Rule Nine/Ten/Six/-Seven processing happens.

2.3 Kelvin versioning

Each version of Nock

telescopic versioning

2.4 Exercises

Compose a Nock interpreter in a language of your choice. (These aren't full Arvo interpreters, of course, since you don't have the Hoon, `%zuse`, and vane subject present.)

Elements of Hoon 3

3.1 Reading the Runes

The goals of this section are for you to be able to:

1. Identify Hoon runes and children in both inline and long-form syntax.
2. Trace a short Hoon expression to its final result.
3. Produce output as a side effect using the `&` rune.

For the first several exercises, we will suggest that you utilize one of these methods in particular so that you get a feel for how each works. After you are more comfortable working with Hoon code on Urbit, we will refrain.

The terminology used is often unfamiliar. Sometimes this means that you are dealing with a truly new concept (and overloading an older word like "subroutine" or "function" would obfuscate), and sometimes you are dealing with an internal aspect that doesn't really map well to other systems. The strangeness can be frustrating. The strangeness can make concepts fresh again. You'll encounter both as you move ahead.

Each rune accepts at least one child, except for `!!` "zapzap".

3.2 Irregular Forms

Many runes in common currency are not written in their regular form (tall or wide), but rather using syntactic sugar as irregular.

For instance, `%-` "cenhep" is most frequently written using parentheses `()` which permits a Lisp-like calling syntax:

```
(add 1 2)
```

is equivalent to

```
%-  add  [1 2]
```

is also equivalent to

```
%-(add [1 2])
```

Hoon parses to an abstract syntax tree (AST), which includes cleaning up all of the sugar syntax and non-primitive runes. To see the AST of any given Hoon expression, use `!,` "zapcom".

```
> !,(*hoon TODO)
TODO
```

Although not a compiled language, the binary tree structure of Hoon can lead to fairly involved programs which are difficult to type and parse as directly as some other languages afford. We instead encourage you to use one of three methods to run Hoon programs:

1. The Dojo REPL, which offers some convenient shortcuts to modify the subject for subsequent commands.
2. A tight loop of text editor and running fakezod.
3. The online interactive sandbox at https://approaching-urbit.comhttps://approaching-urbit.com

3.3 Nouns

All values in Urbit are nouns, meaning either atoms or cells. An atom is an unsigned integer. A cell is a pair of nouns. Since all values are ultimately integers, we need a way to tell different "kinds" (or applications) of integers apart. Enter auras.

Atoms

For what it may be worth, having all integers isn't that different from any other digital machine, built on binary numbers. These all derive ultimately from Gödel numbering as introduced by Gödel in the proof of his famous incompleteness theorems. Urbit makes this about as apparent as C does (via `union`, for instance), but it's first-order accessible via the Dojo REPL.

Atoms have auras which are tagged types. In other words, an aura is a bit of metadata Hoon attaches to a value which tells Urbit how you intend to use a number. (Of course, ultimately an aura is itself an integer as well!) The default aura for a value is `@ud`, unsigned decimal, but of course there are many more. Aura operations are extremely convenient for converting between representations. They are also used to enforce type constraints on atoms in expressions and gates.

For instance, to a machine there is no fundamental difference between binary 0b1101 1001, decimal 217, and hexadecimal 0x*d*9. A human coder recognizes them as different encoding schemes and associates tacit information with each: an assembler instruction, an integer value, a memory address. Hoon offers two ways of designating values with auras: either directly by the formatting of the number (such as `0b1101.1001`) or using the irregular syntax `'@'`:

```
0b1101.1001
'@ud'0b1101.1001  :: yields 217
'@ux'0b1101.1001  :: yields 0xd9
```

Example 3.3.1 Try the following auras. See if you can figure out how each one is behaving.

```
'@ud'0x1001.1111
'@ub'0x1001.1111
'@ux'0x1001.1111
'@p'0x1001.1111

'@ud'.1
'@ux'.1
'@ub'.1
'@sb'.1

'@p'0b1111.0000.1111.0000

'@ta''hello'
'@ud''hello'
'@ux''hello'
'@uc''hello'
'@sb''hello'
'@rs''hello'
```

For a full table of auras, see Appendix **??**.

The atom/aura system represents all simple data types in Hoon: dates, floating-point numbers, text strings, Bitcoin addresses, and so forth. Each value is represented in least-significant byte (LSB) order; for instance, a text string may be deconstructed as follows:

```
'Urbit'
0b111.0100.0110.1001.0110.0010.0111.0010.0101.0101
0b111.0100 0b110.1001 0b110.0010
0b111.0010 0b101.0101
```
116 105 98 114 85 (ASCII characters)
t i b r U

Note in the above that leading zeroes are always stripped. Since each atom is an integer, there is no way to distinguish 0 from 00 from 000 etc.

In this vein, it's worth mentioning that Dojo automatically parses any typed input and disallows invalid representations. This can lead to confusion until you are accustomed to the type signatures; for instance, try to type `0b0001` into Dojo.

Operators . Hoon has no primitive operators. Instead, aura-specific functions or *gates* are used to evaluate one or more atoms to produce basic arithmetic results. Gate names are conventionally prefixed with `++` which designates them as *arms* of a *core*. (More on this terminology in Section **??**.) Some gates operate on any input atom auras, while others enforce strict requirements on the types they will accept. Gates are commonly invoked using a Lisp-like syntax and a reverse-Polish notation (RPN), with the operator first followed by the first and second (and following) operands.

Operation	Function	Example
Addition	`++add`	`(add 1 2)` → `3`
Subtraction	`++sub`	`(sub 4 3)` → `1`
Multiplication	`++mul`	`(mul 5 6)` → `30`
Division	`++div`	`(div 8 2)` → `4`
Modulus/Remainder	`++mod`	`(mod 12 7)` → `5`

Following Nock's lead, Hoon uses loobeans (0 = true) rather than booleans for logical operations. Loobeans are written `%.y` for true, 0, and `%.n` for false, 1.

Operation	Function	Example
Greater than	`++gth`	`(gth 5 6)` → `%.n`
Greater than or equal to	`++gte`	`(gte 5 6)` → `%.n`
Less than	`++lth`	`(lth 5 6)` → `%.y`
Less than or equal to	`++lte`	`(lte 5 6)` → `%.y`
Equals	`=`	`=(5 5)` → `%.y`
Logical `AND`, ^{T}ODO	`&`	`&(%.y %.n)` → `%.n`
Logical `OR`, v	`|`	`|(%.y %.n)` → `%.y`

Operators can be grouped for precedence; *e.g.*,,

TODO

```
1 \&()
```

The Hoon standard library, largely in `%zuse`, further defines bitwise operations, arithmetic for integers and floating-point values (half-width, single-precision, double-precision, and quadruple-precision), TODO These are introduced incidentally as necessary and listed in more detail in Appendix **??**.

Cells

binary tree format flattened representation/convention

Binary trees are explained in more detail in Section **??**.

Hoon values are addressed as elements in a binary tree.

Finally, the most general mold is ∗ which simply matches any noun—and thus anything in Hoon at all.

3.4 Hoon as Nock Macro

The point of employing Hoon is, of course, that Hoon compiles to Nock. Rather than even say *compile*, however, we should really just say Hoon is a *macro* of Nock. Each Hoon rune, data structure, and effect corresponds to a well-defined Nock primitive form. We may say that Hoon is to Nock as C is to assembler, except that the Hoon-to-Nock transformation is completely specified and portable. Hoon is ultimately defined in terms of Nock; many Hoon runes are defined in terms of other more fundamental Hoon runes, but all runes parse unambiguously to Nock expressions.

We call Hoon's data type specifications *molds*. Molds are more general than atoms and cells, but these form particular cases. Hoon uses molds as a way of matching Nock tree structures (including Hoon metadata tags such as auras).

Be careful to not confuse `=(a b)`, which evaluates to `.=`, with the various `?` runes like `?=`.

3.5 Key Data Structures

Lists

Text

Both cords and tapes are casually referred to as strings.

Hoon recognizes two basic text types: the *cord* or `@t` and the *tape*. Cords are single atoms containing the text as UTF-8 bytes interpreted as a single stacked number. Tapes are lists of individual one-element cords.

Lists are null-terminated, and thus so are tapes.

Cords are useful as a compact primary storage and data transfer format, but frequently parsing and processing involves converting the text into tape format. There are more utilities for handling tapes, as they are already broken up in a legible manner.

```
++  trip
  |=  a=@  ^-  tape
  ?:  =(0 (met 3 a))  ~
  [^-(@ta (end 3 1 a)) $(a (rsh 3 1 a))]
```

For instance, `trip` converts a cord to a tape; `crip` does the opposite.

All text in Urbit is UTF-8 (*a fortiori* ASCII). The `@c` UTF-32 aura is only used by `%dill`and Hood (the Dojo terminal agent).

```
++ crip |=(a=tape `@t`(rap 3 a))
```

`++rap` assembles the list interpreted as cords with block size of 2^3 (in this case).

Cores, Gates, Doors

> anyway you can explicitly set the sample in an iron core but you can't use it with +roll New messages below 11:54 (master-morzod) `%gold` is the default, read/write everything; `%iron` is for functions (write to the sample with a contravariant nest check), `%lead` is "hide the whole payload", `%zinc` completes the matrix but has probably never been used `%iron` lets you refer to a typed gate (without wetness), without depending on all the details of the subject it was defined against `%lead` lets you export a library interface but hide the implementation details

Molds

Maps, Sets, Tree

3.6 Generators

Naked Generators

`%say` generators

`%ask` generators

3.7 Libraries

3.8 Unit Tests

3.9 Building Code

Advanced Hoon 4

hard/soft atoms, seeing atoms, etc. TODO

4.1 Cores

Variadicity

Genericity

4.2 Molds

As we saw when discussing auras, molds are the most general category of type in Hoon.

Polymorphism

4.3 Rune Families

4.4 Marks and Structures

4.5 Helpful Tools

See also Section **??** which discusses common "factory patterns" in subject-oriented programming.

4.6 Deep Dives

Text Stream Parsing

JSON Parsing

HTML/XML Parsing

System Development

The Kernel 5

5.1 Arvo

Arvo is essentially an event handler which can coordinate and dispatch messages between vanes as well as emit %unix events to the underlying (presumed Unix-compatible) host OS. Arvo does not carry out several tasks specific to the machine hardware, such as memory allocation, system thread management, and hardware- or firmware-level operations. These are left to the king and serf, or the daemon processes which together run Arvo. Collectively, the system-level instrumentation of Arvo is described in Chapter **??**.

%zuse and %lull

%zuse and %lull define common structures and library functions for Arvo.

subject wrapped

5.2 %ames, A Network

In a sense, %ames is the operative definition of an urbit on the network. That is, from outside of one's own urbit, the only specification that must be hewed to is that %ames behaves a certain way in response to events.

%ames implements a system expecting—and delivering—guaranteed one-time delivery. This derives from an observation by **Yarvin2016** in the Whitepaper: "bus v. commands whatever"

UDP packet structure

network events acks & nacks

5.3 %behn, A Timer

%behn is a simple vane that promises to emit events after—but never before—their timestamp. This guarantee

As the shortest vane, we commend %behn to the student as an excellent subject for a first dive into the structure of a vane.

%behn maintains an event handler and a state.

Any task may have one of the following states:

```
%born   born:event-core
%rest   (rest:event-core date=p.task)
%drip   (drip:event-core move=p.task)
%huck   (huck:event-core syn.task)
%trim   trim:event-core
%vega   vega:event-core
%wait   (wait:event-core date=p.task)
%wake   (wake:event-core error=~)
```

5.4 %clay, A File System

++ford, A Build System

Scrying

Marks and conversions

5.5 %dill, A Terminal driver

5.6 %eyre and %iris, Server and Client Vanes

5.7 %jael, Secretkeeper

%jael weighs in as one of the shorter vanes

%jael is named after Jael, the wife of Heber, who kept mum and slew fleeing enemy general Sisera in Judges 4.

As of Arvo XXX K, the

5.8 Azimuth, Address Space Management

Urbit HD wallet

Comet keys . Comets do not have an associated Urbit HD wallet, and their keys work slightly differently.

> yeah thats how comet mining works. so you'd just put the private key you generated for a comet on the card, and this would be the ames DH exchange private key. i suppose you could still obfuscate it with a master ticket @q, by just picking a 128 bit hash, but it would be used differently than a normal azimuth master key, which is a @q used to derive a bunch of ethereum wallets private keys (and ultimately the initial network key, but that isnt required). 9:15 >and yeah whether a key works at the time it is mined is dependent on whether the routing node automatically assigned to the comet public key is currently working > lagrev-nocfep: the comets name is its public key

5.9 The Hoon Parser

Userspace 6

6.1 `%gall`, A Runtime Agent

Factory Patterns

6.2 Deep Dives in `%gall`

Each of the following case studies is drawn from published code, most of it incorporated into the Urbit userspace. In some cases, the original code uses conventions we have not yet introduced; we have simplified these to rely on the runes introduced in the main text through Chapter **??**.

Chat CLI

Drum and Helm

Bitcoin API

Bots

6.3 Threading with Spider

6.4 Urbit API

6.5 Deep Dives with Urbit API

Time (Clock)

Publish

`%graph-store`

Modern `%gall` is sometimes called "static Gall" in contrast to an earlier specification "dynamic Gall." Dynamic Gall did not specify the arms and permitted each agent its own structure; in practice, this proved to be difficult for programmers to maintain in a consistent manner, leading to code refactors and maintenance of default arms (for backwards compatibility) of agents.

Supporting Urbit 7

7.1 Booting and Pills

7.2 %unix Events

7.3 Nock Virtual Machines

++mock

King and Serf Daemons

Vere (Reference C Implementation)

King Haskell (Haskell Implementation)

Jaque (JVM Implementation)

7.4 Jetting

Jet matching and the dashboard

Concluding Remarks 8

8.1 Booting and Pills

Appendix

Appendices A

A.1 Comprehensive table of Hoon runes

A.2 Hoon versions

A.3 Nock versions

A.4 Hoon comparison with other languages

A.5 `%zuse`/`%lull` versions

A.6 Textbook changelog