NARCISSUS: Deriving Correct-By-Construction Decoders and Encoders from Binary Formats

Sorawit Suriyakarn
Clément Pit-Claudel
MIT CSAIL
{sorawit, cpitcla}@csail.mit.edu

Benjamin Delaware
Purdue University
bendy@purdue.edu

Adam Chlipala
MIT CSAIL
adamlc@csail.mit.edu

Abstract
Every injective function has an inverse, although constructing
the inverse for a particular injective function can be quite
tricky. One common instance of inverse-function pairs is the
binary encoders and decoders used to convert in-memory
data into and out of a structured binary format for network
communication. Ensuring that a given decoder is a proper
inverse of the original encoder is particularly important, as
any error has the potential to introduce security vulnerabilities
or to corrupt or lose data in translation.

In this paper, we present a synthesis framework, NARCI-
SUS, that eliminates both the tedium and the potential for
error in building the inverse of a binary encoder. The start-
ing point of the process is a binary format, expressed as a
functional program in the nondeterminism monad, that pre-
cisely captures all the valid binary encodings of an arbitrary
datatype instance. From this specification, NARCISSUS syn-
thesizes a decoder that is guaranteed to be the inverse of this
relation, drawing on an extensible set of decoding strategies
to construct the implementation. Each decoder is furthermore
guaranteed to detect malformed encodings by failing on in-
puts not included in this relation. The derivation is carried
out inside the Coq proof assistant and produces a proof trail
certifying the correctness of the synthesized decoder. We
demonstrate the utility of our framework by deriving and
evaluating the performance of decoders for all packet formats
used in a standard network stack.

1. Introduction
The code responsible for encoding and parsing external data
is a vital component of any software that communicates with
the outside world: failure to produce or correctly interpret
encoded data that conform to a standard format can result in
lost or corrupted data, while bugs in the decoder code that
takes untrusted external data as input represents a key at-
tack surface for malicious actors. Writing code that conforms
to a high-level format description by hand is both tedious
and error-prone. As one example, a bug in a seldom-used
piece of the parser for IP headers used by the network stack
of MirageOS [12] was only discovered and patched three
months ago. Code-generation frameworks that synthesize
encoders and decoders from high-level data-description lan-
guages [4, 7–9, 13] are a particularly appealing solution to
this problem, offering both convenience and (potentially)
higher-assurance code. While this approach removes the
threat of programmer-introduced errors in the communication
code, it forces the user to trust that the code-generation frame-
work is correct. Frameworks are also constrained by their
data-description language, potentially limiting their applica-
tion to standardized formats. To address this latter problem,
frameworks like Nail [4] allow for user-defined extensions to
the code generator.

Unfortunately, extensibility comes at the cost of increasing
the trusted code base: there is no guarantee that a user-defined
extension does not introduce errors into either the decoder
or encoder, violating conformance with the data format or
introducing security vulnerabilities. This paper presents a
framework, NARCISSUS, that solves both problems: it is both
extensible, in that users can freely add new data formats to the
specification language, and sound, in that every synthesized
decoder and encoder is accompanied by a mechanized proof
of correctness, checked by the Coq proof assistant [20],
regardless of any user-defined extensions.

Input formats to NARCISSUS are specified as arbitrary
injective binary relations between source data and its encod-
ing in Coq’s higher-order logic, allowing rich user-defined
encoding strategies. From this specification, NARCISSUS syn-
thesizes decoder functions that are guaranteed to both cor-
rectly invert the input specification and detect any malformed
packet not conforming to the specified format. NARCISSUS
consists of a small set of core definitions and provides a
library of common binary formats and decoder implemen-
tation strategies that can be freely and safely extended by users, with nothing distinguishing user-provided components from those included in the library. The synthesis process is also extensible, in that users can add their own implementation strategies without breaking our correctness guarantees. This entire framework is realized in the Coq proof assistant, yielding a high degree of confidence in the derived code.

We evaluate the expressiveness of NARCISSUS by deriving decoders for several standard networking protocols, highlighting any protocol-specific extensions required. We furthermore evaluate the functionality and performance of the synthesized code by incorporating it into the networking stack of MirageOS [12].

1.1 Motivating Example

As a motivating example of NARCISSUS in action, consider the resource records used by hosts to respond to client queries in the domain name system, shown in Figure 2. Each field of this record has a different type: the name field holds the owner of the record as a list of labels, the class field is an enumerated type holding the protocol associated with the record (almost always Internet these days, as it is quite difficult to find CHAOS nodes), the ttl field holds a 32-bit word specifying the lifetime of the record for clients wanting to cache a response, and the rdata field is a variant type holding different kinds of information for the domain, e.g. an address, the authoritative server for a domain, or host information for the domain. This relatively simple example already illuminates some of the intricacies involved in both specifying and writing a correct decoder.

Importantly, the binary format for encoding these records, also shown in Figure 2, has been established for three decades [14], highlighting the need for NARCISSUS to be flexible enough to express existing protocols. The correctness criteria for the ttl and class fields are straightforward: our framework simply needs to ensure that the encoder and decoder agree on both the endianness used in ttl and the codes used for the enumerated type in the class field (and furthermore conform to the protocol specification), but the rdata fields require more subtle criteria. In order to properly decode the rdata field of a packet, the format specifies that two additional pieces of information be encoded alongside the resource records fields: a TYPE tag that dictates which variant type should be used when decoding the RDATA portion of the packet, and the RDLENGTH flag which is used to tell when to stop decoding certain types of resource data. Thus, the correctness of the decoder for rdata depends on previously decoded bits of information (which must have been decoded correctly themselves).

Furthermore, DNS packets use a novel form of compression for domain names, complicating the encoding of the name field: a domain name is either directly encoded as a list of labels terminated by a zero octet or as a (possibly empty) list of labels terminated by a pointer to the location of a previously encoded domain name. Thus, the domain

```
| NAME |
| 0 1 2 3 4 5 6 7 |
| TYPE |
| 0 1 2 3 4 5 6 7 |
| CLASS |
| 0 1 2 3 4 5 6 7 |
| TTL |
| 0 1 2 3 4 5 |
| RDLENGTH |
| 0 1 2 3 |
| RDATA |
```

![Figure 2](image_url)
name conf.researchr.org could be encoded by either encoding the character strings conf, researchr, org, and the terminal character; or by encoding conf followed by a specialized pointer to the offset of a previous appearance of researchr.org in the packet. The peculiarities of this compression strategy highlight the need of our framework to be not only extensible, but extensible in a correctness-preserving manner, that is, the framework should provide a strong guarantee that any user-provided extensions do not break our (as-of-yet unspecified) correctness properties. In order to do this, the framework may need to maintain invariants between the internal state of both the encoder and decoder (in the case of our example, that the cache used by both of them points to the correct location of previously seen domains). The DNS compression strategy points to another challenge, this time with respect to our specification of decoder correctness: since a domain name can be encoded in several different ways depending on if and where compression is used, there is no canonical encoding of a DNS packet according to the standard. Thus, a correct decoder is not the inverse of a single encoder function; rather it is the inverse of an encoding relation that specifies all the valid encodings of a particular data type.

This is precisely the intuition behind our approach to the derivation of correct-by-construction binary decoders, as illustrated in Figure 1. The first step is to capture the valid binary formats of a datatype as the possible outputs of a nondeterministic program, where different encodings are represented as a nondeterministic choice among available encoding strategies. encode_RRecord in Figure 2 is an example of such a nondeterministic encoder for DNS resource records. It is built up with a combination of formats for basic datatypes drawn from the core library, i.e. encodeW and encode_enum, and format combinator, i.e. ThenC and DoneC, for building up larger decoders from these building blocks. Users can freely include their own formats, written as nondeterministic programs, in this specification; encode_DomainName, the encoder for domain names used in encode_RRecord, is an example of such a user-provided extension.

A correct decoder is one that inverts this relation, precisely mapping any element in the set of bytestrings specified by such a format back to the member of the original datatype that generated it, and failing if the binary string does not fall in the set of valid encodings. The ValidDecoder type-level function used to define decoders is effectively the dependent pair of a decoder with a proof that it meets this specification; NARCissus frames the derivation of a correct-by-construction decoder as the interactive search for an inhabitant of this type à la decode_RRecord. The framework automates the search for an inhabitant of this type using the synthesize_decoder tactic, which can be extended with user-defined decoder implementation strategies. In the derivation of decode_RRecord in Figure 2, for example, these strategies are passed to this tactic as DomainName_Hints. The decoder functions synthesized by this tactic can then be extracted to OCaml via Coq’s extraction mechanism.

We pause here to recap the features of NARCissus that distinguish it from existing frameworks:

- In contrast to interface generators, including XDR [19], ASN.1 [7], Apache Avro [1], and Protocol Buffers [21], where the tool decides the encoding format from a logical description of the source data, NARCissus provides fine-grained control over the precise shape of encoded data used in the binary relation specifying a format.
- The specification language in NARCissus is that of Coq’s higher-order logic, and can be extended with new, user-defined formats, in contrast to traditional parser generators such as YACC [10], ANTLR [16], and binpac [15] with fixed input languages.
- NARCissus is foundational, in that it has a small core of trusted definitions: the base library of format specifications and decoder implementation strategies are components on top of this core. Other data-description frameworks, including PADS [8], PacketTypes [13], and Datascript [2], do not directly support user-defined language extensions and require modifying the large code base of the tools themselves.
- Finally, even those frameworks that easily support user-defined extensions, like Nail [4], provide no guarantees about the safety of those extensions. In contrast, NARCissus is sound, providing a machine-checked proof that even decoders built using user-defined extensions are correct by construction.

The rest of this paper is structured as follows: Section 2 describes the nondeterministic programs we use to specify datatype formats. Section 3 gives a precise specification for correct decoders. Subsection 3.1 describes how we package decoding strategies into composable building blocks. Section 4 describes the synthesize_decoder tactic for deriving correct-by-construction decoders, while Section 5 illustrates how an IP Checksum component is added to the library. Section 6 evaluates NARCissus via the synthesis of decoders for several standard binary formats, and Section 7 finishes with a discussion of related work.

2. Specifying Binary Formats

In NARCissus, a binary encoder is a function from an arbitrary data type T to an encoded representation in the type S of byte strings. Such a function is typed like encoder : T → S, while a decoder is the inverse function that transforms the encoded representation back into the original type: decoder : S → T. Section 3 describes precisely the desired relationship between the encoder and decoder. Our framework uses an abstract data type (ADT) for bit strings, S, which is effectively a queue equipped with an append operator ++ to abstract the concrete details of the encoded representation from the
ADT $S$
\[
\text{Definition } \text{id} : S; \\
\text{Definition } ++ : S \rightarrow S; \\
\text{Definition } \text{enqueue} : B \rightarrow S \rightarrow S; \\
\text{Definition } \text{dequeue} : S \rightarrow \text{option} (B \times S);
\]
\[
\text{Axiom } \text{app}_{\text{id}} \text{left} : \exists s_1, id \leftrightarrow ++ s_1 = s_1; \\
\text{Axiom } \text{app}_{\text{id}} \text{right} : \exists s_1, s_2 \leftrightarrow ++ s_1 = s_1; \\
\text{Axiom } \text{app}_{\text{assoc}} : \forall s_1, s_2, s_3 \leftrightarrow (s_1 ++ s_2) ++ s_3 = s_1 ++ (s_2 ++ s_3); \\
\text{Axiom } \text{dequeue}_{\text{app}} : \forall b \leftrightarrow s_1 s_2, \text{dequeue \_ s_1} = \text{Some} (b, s_2) \rightarrow \text{dequeue \_ s_2} = \text{Some} (b, s_3) \leftrightarrow s_1 ++ s_3; \\
\text{Axiom } \text{enqueue}_{\text{app}} : \forall b \leftrightarrow s_1 s_2, \text{enqueue \_ b \_ s_1} = \text{Some} (b, s_2) \leftrightarrow \text{dequeue (enqueue \_ b \_ id)} = \text{Some} (b, \text{id}); \\
\text{Axiom } \text{dequeue}_{\text{id}} : \forall b \leftrightarrow s_1 s_2, \text{dequeue \_ s_1} = \text{Some} (b, s_3) \rightarrow \text{dequeue \_ s_2} = \text{Some} (b, s_3) \leftrightarrow s_1 = s_2
\]

Figure 3. The interface of the BitString ADT used for encoded data, with some length operations elided.

As an example, we can specify the encoding of the type-of-service field in the original specification of IPv4 by appending two nondeterministically chosen bits onto the six-bit word in the type-of-service field used by a packet ip:
\[
x \leftarrow \{ b : \text{word2 | True } \}; \text{return} (x ++ \text{ip!"ToS"})
\]

In addition to allowing NARCISSUS to capture formats with more than one valid encoding per source datatype, using the nondeterminism monad has the virtue of enabling more declarative specifications of encoders, which can in turn make it easier to prove the soundness of the corresponding decoder. As an example, consider how the following nondeterministic function separates the leftmost label in the domain name domain for encoding before processing the remaining labels in the domain$^1$:
\[
\text{split domain} := \{ (\text{label}, \text{domain}') \mid \text{ValidLabel label} \land \text{domain} = \text{label} ++ \text{"."} ++ \text{domain}' \land \text{ValidLabel label} \land \text{domain}' = \text{"."} \}
\]

There is no nondeterminism in this set, in the sense that it includes (at most) a single element, but it allows an encoder specification to capture the essential functionality of a split function. A particular encoder can guarantee that this set will be inhabited by limiting domain to be a valid domain name, as we will see in subsequent sections. The nondeterminism monad can also conveniently express recursive formats without worrying about termination via a fixpoint combinator, FixComp, using the standard definition of the intersection of all sets closed under a generator function:
\[
\text{FixComp } f = \{ x \mid x \in f x \}
\]

Combining these two definitions enables a succinct specification of the format of (uncompressed) domain names:
\[
\text{encodeDN} \text{ domain} = \text{\text{FixComp (\lambda rec. if domain = "then return id else (label, domain') \leftarrow split domain; s_1 \leftarrow encodeLabel label; s_2 \leftarrow rec domain'; return (s_1 ++ s_2) ).}}
\]

In order to enable encoders to utilize internal state, we layer the state monad on top of the nondeterminism monad to create the full signature for binary formats used by NARCISSUS:
\[
\text{encoderSpec} : A \rightarrow \Sigma \rightarrow \text{Comp} (S \times \Sigma)
\]

The type $\Sigma$ is a parameter of the framework, corresponding to whichever type of state a particular format requires. Figure 4 gives the specifications of encoders for fixed-length interpretations as set operations:
\[
\text{return } v \triangleq \{ v \} \\
\{ x \mid P x \} \triangleq \{ x \mid P x \}
\]

1. The ValidLabel predicate ensures that label does not contain invalid characters, such as ".".
Def encode_{\text{words}} (w : \text{Words}) (\sigma : \Sigma) :=
FixComp (\lambda \text{rec. match} w \text{ with}
| \text{WO} \Rightarrow \text{return} (\sigma, \text{id})
| \text{WS b w'} \Rightarrow \text{return} \text{rec w'} (\text{enqueue b} \, s) \, \sigma
\text{end}).

Def encode_{\text{Nat}} (n : \text{Nat}) (\sigma : \Sigma) :=
encode_{\text{WtoN16}} (n) \, \sigma .

Def encode_{\text{List T}} (l : \text{List T}) (\sigma : \Sigma) :=
FixComp (\lambda \text{rec. match} l \text{ with}
| [] \Rightarrow \text{return} (\sigma, \text{id})
| a :: l' \Rightarrow (s_1, \sigma) \leftarrow \text{encoder}_{\text{T}} \, a \, \sigma ;
(s_2, \sigma) \leftarrow \text{rec l'} \, \sigma ;
\text{return} (s_1 :: s_2, \sigma)
\text{end}).

Def encode_{\text{ListTerm T}} (t : \text{ListTerm T}) (\sigma : \Sigma) :=
FixComp (\lambda \text{rec. match} t \text{ with}
| [] \Rightarrow \text{encoder}_{\text{T}} \, t \, \sigma
| a :: l' \Rightarrow (s_1, \sigma) \leftarrow \text{encoder}_{\text{T}} \, a \, \sigma ;
(s_2, \sigma) \leftarrow \text{rec l'} \, \sigma ;
\text{return} (s_1 :: s_2, \sigma)
\text{end}).

Figure 4. Encoder specifications for fixed-length words and variable-length polymorphic lists with and without a terminal code.

In addition to formats for base datatypes, the base library of ARCISSUS includes two encoder combinators for encoding more complex data, presented in Figure 5. The first of these, \text{ThenC}, sequences the results of two encoders, while \text{DoneC} syntactically signifies the end of the encoded bit string. The specification of an encoder for a list of the resource records from Figure 2 can be built up using these combinators and a function \text{NToW16} from natural numbers to 16-bit words:

Def encodeRRs (l : \text{List ResourceRecord}) :=
encode_{\text{List}} \text{NToW16} \, l \, \text{ThenC}
\text{DoneC}.

Intuitively, the formats for base datatypes and the format combinators make up the core of an embedded domain-specific language for building up formats representing binary relations between input data and bit strings. Users can, of course, incorporate their own syntax for base formats or combinators into this EDSL by providing denotations for their extensions.

**Deriving Binary Encoders** A correct encoder is one that maps every instance of the source datatype to a bit string falling into the set described by a format:

Def EncodeCorrect (T) (encoderSpec : T \rightarrow \Sigma \rightarrow \text{Comp} (\Sigma \times \Sigma))
Def compose (encode_1 : \Sigma \rightarrow \text{Comp} (\Sigma \times \Sigma))
(encode_2 : \Sigma \rightarrow \text{Comp} (\Sigma \times \Sigma)) (\sigma : \Sigma) :=
(\sigma) \leftarrow \text{encode}_1 \, \sigma ;
(\sigma) \leftarrow \text{encode}_2 \, \sigma ;
\text{return} (s_1 :: s_2, \sigma).

Given the specification of a format, it is possible to automatically derive a correct-by-construction implementation by iteratively refining the specification using a set of refinement rules à la the Fiat framework [5].

### 3. Specifying Binary Decoders

Before diving into the precise definition of decoder correctness used by ARCISSUS, we consider the high-level properties that such a “correct” decoder should satisfy. Given the specification of a binary format as a nondeterministic function \text{encoderSpec}, a correct decoder \text{decode} must clearly be a left inverse of \text{encoderSpec}, i.e. \text{decode} must map every element \text{s} in the image of \text{t} of \text{encoderSpec} back to \text{t}:

\text{decodeCorrect}_1 \, \text{encoderSpec} \, \text{decode} \triangleq 
\forall \, t, \, s, \, s' \in \text{encoderSpec} \, t \, \text{decode} \, s = t

Less clear is what \text{decode} should do with bit strings that do not fall into the set allowed by the format: should the decoder fail on such inputs, or should its behavior be unconstrained? In the interest of detecting malformed and potentially malicious inputs, ARCISSUS takes the former approach, requiring that a correct decoder be a partial function that only translates correctly encoded data:

\text{decodeCorrect}_2 \, \text{encoderSpec} \, \text{decode} \triangleq 
\forall \, t, \, s, \, s' \in \text{encoderSpec} \, t \, \text{decode} \, s = t

While the rest of this paper focuses on deriving decoders satisfying both criteria, our approach also straightforwardly applies to the synthesis of decoders only satisfying the first criterion, in the case that users choose to sacrifice strict format validation for efficiency.

We can now identify the precise signature of decoders in ARCISSUS. An important design element of the framework is to treat decoders as consumers of the queue provided by the bit string ADT. In other words, a decoder decodes some portion of the head of the bit string and returns the rest alongside a decoded value, as shown in the decoder corresponding to \text{encode}_{\text{words}} from Figure 4:

Def decode_{\text{words}} (s : \Sigma) (\sigma : \Sigma) :=
match \text{n} \text{ with}
| 0 \Rightarrow \text{return} (\text{WO}, \, s, \, \sigma)
| s \, n' \Rightarrow (b, \, s') \leftarrow \text{dequeue} \, s;
Def decode' (s : S) (σ : Σ) :=
(w, s', σ') ← decodeW 16 s σ ;
return (W16ToN w, s', σ')

Def decode_List {T} (decodeT : S → Σ → Comp (T × Σ × S)) n (s : S) (σ : Σ) :=
machine n with
| O ⇒ return (nil, s, σ)
| S n' ⇒ (t, s', σ') ← decodeT t s σ ;
{| (l, s', σ') ← decode_List t' s' σ' ;}
return (t : l, s', σ').

Figure 6. Decoders for the binary formats from Figure 4.
(w, s') ← decodeW n s σ ;
return (WS b w, s', σ')

As shown above, decoders are also monadic functions, although in contrast to encoder functions, they combine the state monad with the option (failure) monad in order to model the partiality of decoders. In decodeW, for example, should a dequeue fail because s is empty, the entire decoder will terminate with an error value. Thus, the complete signature for a decoder for a datatype T in our framework is:

decodeT : S → Σ → Option (T × S × Σ)

Figure 6 shows the decoders for the other binary formats. Even these simple types demonstrate that the decoders are more complicated than the corresponding encoders, precisely because they do not have a full view of the original data. In the case of decode_List, for example, the decoder takes the number of iterations as input; in order for a compound decoder using this function to be correct, it needs to be able to recover this parameter prior to decoding the list. For a decoder for the binary format specified by encodeRRs, for example, does precisely this:

Def decodeRRs (s : S) (σ : Σ) :=
(n, s', σ') ← decodeW s σ ;
decode_List decode_RRecord n s σ .

Before giving the complete definition of decoder correctness, we note that it is often convenient to condition it on two additional assumptions. Firstly, the statement restricts the data being encoded via a predicate in order to only consider well-formed input, i.e. DNS packets that only have valid domain names or trees that have been normalized. A similar result could be achieved by using subset types as the source datatype in lieu of an extra assumption, but externalizing the well-formedness condition frees NARCISSUS from having to worry about subtleties of dependent typing. Furthermore, this predicate is a natural means for retaining information about previously parsed data when verifying decoder combinators, as we will see in the next section. Secondly, the statement requires that decoders are run in appropriate states via relations between the state used to encode the data and the state used by the decoder. Finally, NARCISSUS defines the judgment of decoder correctness with respect to a binary format as a quaternary relation on a state relation Q, a data predicate P, a binary format encode, and a decoder function decode:

Q, P ⊢ decode :=
∀ (σE : σE : ΣE) (σD : σD : ΣD) (data : A) (s s' : S),
Q σE σD → P data →
∃ σE σD, decode (s + s') env' = Some (data, s', σD')
∧ Q σE σD →
decode s σD = Some (data, s', σD') →
∃ s' σE : σE : ΣE, (s', σD') ∈ encode data σE
∧ s = s' + + s ∧ P data ∧ Q σE σD'.

3.1 Building Decoding Strategies

Figure 7 presents the correctness rules for decodeW and the decoders in Figure 6. NATCORRECT has the first example of a data predicate, constraining the natural numbers that can be safely encoded and decoded using encodeW and decodeW to those that can be stored in a byte. While both decodeW and decode_List recurse over the lengths of the datatype they are decoding, they are distinguished by how this parameter is encoded in the binary format. NARCISSUS uses length-indexed words, that is, the number of bits in a word is encoded in its type, so the length parameter used by decodeW is completely determined by the type of data being decoded. Since most formats use fixed-length words, this length parameter is embedded in the format itself. Contrast this with decode_List, where the length is not fixed by the data type: here we rely on a predicate relating the list length to the parameter n passed to decode_List: |l| = n. Note that the variable l is the argument of the data predicate and stands in for any list used in the correctness judgment. Thus, we are not able to pass |l| as an argument to decode_List, rather this length must be recovered by, for example, encoding it in the format as well. This may in turn limit the length of the list itself, depending on the encoder used for this value. decode_ListTerm does not require such a parameter, as its correctness rule hinges on another condition: the data predicate stipulates that the terminal character must not be in the encoded list, allowing the decoder to determine when the end of the list has been reached. Finally, we note that the correctness of both decode_List and decode_ListTerm depend on the correctness of the decoder used for list elements decodeT and require that each element of the list satisfies the predicate P σ used in the proof of correctness.

State Predicates The encoders and decoders referenced in Figure 7 are pure, so each corresponding correctness rule is
This relationship is embodied in the correctness rule for a record or the length of a list, before encoding the rest of the version numbers in an IP packet. The first format in C uses a projection function, \( \pi_B \), to encode some partial view of the full datatype \( a \), e.g. a particular field of a record or the length of a list, before encoding the rest of \( a \). The decoder for the compound format first uses a decoder for the domain of \( \pi_B \), \( \text{decode}_B \), to recover \( \pi_B \ a \) before processing the rest of the bit string using a decoder, \( \text{decode}_A \), which takes the decoded \( \pi_B \ a \) as input.

The validity of \( \text{COMPOSECORRECT} \) depends on how it threads information about the projection of the encoded data through its three hypotheses. The first hypothesis establishes that \( \text{decode}_B \) is a correct decoder for \( \text{encode}_B \) under some data predicate \( P_B \); the second states that this predicate holds for any projection from data \( a \) which satisfies the predicate used by the composite decoder \( P_A \). Taken together, these two hypotheses establish that \( \text{decode}_B \) safely recovers the data encoded in the first piece of the format, which is then available to \( \text{decode}_A \) when parsing the rest of the string. The proof that the rest of the string is correctly decoded is captured by the final hypothesis of \( \text{ComposeCorrect} \), which is quantified over an arbitrary value of this parameter, \( b \). The hypothesis augments the proof of correctness for \( \text{decode}_A \) with two pieces of information relating \( b \) to the data obtained from the first part of the format. Firstly, the correctness of \( \text{decode}_B \) ensures that its data predicate holds for \( b \): \( P_B \ b \). Secondly, recall that the statement of \( \implies \) is quantified over an arbitrary piece of data, \( a \), constrained by a predicate \( P_A \); we include the knowledge that \( b \) was derived from \( \pi_B \ a \) into the proof of \( \text{decode}_A \) by augmenting its data predicate with this fact: \( \lambda a. \ P_A a \land \pi_B a = b \).

In contrast, the identifier \( b \) used in \( \text{COMPOSECORRECTNO} \) is a constant that is independent of the original data. This rule avoids polluting the data predicate in the proof of correctness for \( \text{decode}_A \) with an extraneous clause, at the cost of proving that the data predicate \( P_B \) used by \( \text{decode}_B \) holds for this constant. In order to ensure that the encoded bit string parameterized over an arbitrary relation \( Q \) between encoder and decoder states. For an example of a more constrained rule, recall the format for domain names, \( \text{encode_DomainName} \), discussed in Subsection 1.1. \( \text{encode_DomainName} \) compresses domain names by using a map from previously seen domain names to their locations in the bit string in order to (potentially) replace repeated domain names with a pointer to that location. The corresponding decoder \( \text{decode_DomainName} \) maintains a map from previously parsed locations to domain names; this map needs to be aligned with the one used in the format in order for this decoder to be correct. This relationship is embodied in the correctness rule for \( \text{decode_DomainName} \):

\[
\lambda \sigma_E \sigma_D. \forall p. \sigma_E p = n \iff \sigma_D n = p. \text{ValidDomain} \vdash \\
\text{encode_DomainName} \implies \text{decode_DomainName} \quad (\text{DOMAINNAMECORRECT})
\]

### 3.2 Decoder Combinators

We now turn to the rules for building correct decoders for the \( \text{ThenC} \) combinator used to sequence two encoders. These rules, shown in Figure 8, allow framework users to derive a valid decoder for a complex format by finding correct decoders for each subformat. Of the two rules for \( \text{ThenC} \), \( \text{COMPOSECORRECT} \) handles the case when the second decoder depends on the output of the first, while \( \text{COMPOSECORRECTNO} \) handles the case when the two decoders are independent. The latter rule is useful for decoding fixed formats which do not depend on the object being encoded, e.g. the version numbers in an IP packet. The first format in \( \text{COMPOSECORRECT} \) uses a projection function, \( \pi_B \), to encode the rest of the bit string using a decoder, \( \text{decode}_B \), which takes the decoded \( \pi_B \ a \) as input.

The validity of \( \text{COMPOSECORRECT} \) depends on how it threads information about the projection of the encoded data through its three hypotheses. The first hypothesis establishes that \( \text{decode}_B \) is a correct decoder for \( \text{encode}_B \) under some data predicate \( P_B \); the second states that this predicate holds for any projection from data \( a \) which satisfies the predicate used by the composite decoder \( P_A \). Taken together, these two hypotheses establish that \( \text{decode}_B \) safely recovers the data encoded in the first piece of the format, which is then available to \( \text{decode}_A \) when parsing the rest of the string. The proof that the rest of the string is correctly decoded is captured by the final hypothesis of \( \text{ComposeCorrect} \), which is quantified over an arbitrary value of this parameter, \( b \). The hypothesis augments the proof of correctness for \( \text{decode}_A \) with two pieces of information relating \( b \) to the data obtained from the first part of the format. Firstly, the correctness of \( \text{decode}_B \) ensures that its data predicate holds for \( b \): \( P_B \ b \). Secondly, recall that the statement of \( \implies \) is quantified over an arbitrary piece of data, \( a \), constrained by a predicate \( P_A \); we include the knowledge that \( b \) was derived from \( \pi_B \ a \) into the proof of \( \text{decode}_A \) by augmenting its data predicate with this fact: \( \lambda a. \ P_A a \land \pi_B a = b \).

In contrast, the identifier \( b \) used in \( \text{COMPOSECORRECTNO} \) is a constant that is independent of the original data. This rule avoids polluting the data predicate in the proof of correctness for \( \text{decode}_A \) with an extraneous clause, at the cost of proving that the data predicate \( P_B \) used by \( \text{decode}_B \) holds for this constant. In order to ensure that the encoded bit string
conforms to the format, per the second clause of \( \text{decode} \), the decoder must check that the decoded constant is equal to \( b \), via the if \((b' = b)\) then ... else ... expression in the decoder.

The final rule presented in Figure 8, \( \text{DONECORRECT} \), finishes the proof for a decoder for a format terminated by \( \text{DoneC} \). It may appear that this rule can only be used for decoders of a single fixed value, since its sole hypothesis stipulates that the data predicate \( P_A \) requires that the encoded data must be some constant \( a' \). As discussed above, however, \( P_A \) accumulates additional constraints when parsing formats built up using \( \text{ThenC} \). Thus, a proof terminated with \( \text{DONECORRECT} \) will include constraints relating the encoded data to all of the previously parsed views of that data. Assuming that the binary format includes enough information to uniquely identify the original data, the constraints in \( P_A \) will force the decoded data to be exactly that used to generate the original bytestring, ensuring the correctness of the full decoder.

One important feature of the decoder in \( \text{DONECORRECT} \) is the conditional validating the data predicate \( P_A \), as required by \( \text{if} \) if \( P_A \) \( a' \) \( \text{then} \ldots \text{else} \ldots \) \( \text{2} \). When \( P_A \) follows immediately from the binary format, e.g. the length of any list decoded by \( \text{decodeList} \) must be less than the maximum value that can be encoded by the format used for its length, this conditional can be discarded via partial evaluation (indeed, our automation removes trivial conditionals in just this manner). If the predicate is more restrictive, for example requiring that a list hold fewer than five elements while using a byte to encode the length, the decoder must check that the data is well-formed.

Figure 9 gives an example application of \( \text{COMPOSECORRECT} \) and \( \text{DONECORRECT} \) in a proof of correctness for a binary format that formats a list of at most \( 2^{10} \) bytes as a sixteen-bit word encoding its length followed by the sequence of bytes in the list:

\[ \begin{array}{cccccccccc}
0 & 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\
\hline
| & \text{LENGTH} & | \\
\hline
| & \text{BYTESTRING} & | \\
\hline
\end{array} \]

The leaves of the proof trees consist of rules for basic data types (natural numbers and lists) and the \( \text{DONECORRECT} \) rule which finishes the proof. The leftmost leaf uses \( \text{NatCorrect} \), requiring that the encoded length fit into a sixteen-bit word. Although this is different from the predicate used by the overall format, the second clause of \( \text{COMPOSECORRECT} \) ensures that this condition holds. A similar weakening step occurs in the other application of \( \text{COMPOSECORRECT} \), where the trivial condition on the elements of the encoding needed by \( \text{LISTCORRECT} \), \( \forall r \in \ell, T r \), is dropped from the data predicate. Observe that the data predicate used in the proof trees for the right branch of \( \text{ThenC} \) is augmented with information about the parsed string as the proof proceeds, so that when the proof reaches the end of the format, the predicate dictates that the length of the encoded string be the result of the initial decoder function, \( |\ell| = n \), and the encoded list be the result of the second decoder \( \ell = l \). This predicate constrains the encoded datatype to be exactly \( l \), allowing the decoder to reconstitute the initial list from the data it has decoded. While the last two clauses in the predicate are guaranteed by the format, the decoder still needs to check that \( l \) meets the original length requirements via the if \( |l| < 2^{10} \) \( \text{then} \) \ldots \text{else} \ldots \) statement. Of course, if this check is too restrictive, the user could relax the initial data predicate to \( |l| < 2^{16} \), as guaranteed by the format, allowing this statement to be simplified away.

Figure 10 includes a complete list of the components currently included in \( \text{NARCISSUS} \). As may be expected, the lines of proof needed to verify \( \text{H} \) typically outnumber the
4. Deriving Correct-By-Construction Decoders

**NARCISSUS** frames the decoder-synthesis problem as a user-guided search for both a decoder function for the encoded type and a proof that it is correct with respect to a specified format. We define a type alias, `CorrectDecoderFor`, previously seen in Figure 2, that packages these two terms together as a dependent pair. `CorrectDecoderFor` is parameterized over the state predicate `StateOK`, the data predicate `DataOK`, and the format specification `FormatSpec`.

**Definition** `CorrectDecoderFor StateOK DataOK FormatSpec :=`  
\[ \Sigma \text{decode. StateOK, DataOK } \vdash \text{FormatSpec } \vdash \text{decode.} \]

**NARCISSUS** includes a tactic `synthesize_decoder` for automatically finding inhabitants of `CorrectDecoderFor`. The behavior of this tactic is broken into three phases:

**Format Normalization** This initial phase unfolds the identifiers of the parameters to `CorrectDecoderFor`, uses the monad laws to normalize the format specification, simplifies the resulting term, and caches any string constants via an OCaml plugin to minimize the size of intermediate proof terms in order to speed up the rest of the derivation.

**Syntax-Directed Search** The main body of the tactic searches for an initial decoder implementation by repeatedly applying \( \leftarrow \text{lemmas. This search consists of a series of rules, triggered on the syntax of the current format in the goal. In addition to specifying which lemma to apply, these rules also attempt to discharge any hypotheses dealing with data invariants via a hint database. The rule for `COMPOSECORRECT`, for example, tries to automatically show that the data invariant for the compound decoder entails the data invariant used by the first decoder by using this database. The most interesting of these rules is the one that tries to finish a derivation by applying `DONECORRECT`. This rule produces two proof obligations: showing that the original data can be completely reconstituted using previously parsed data, and finding a decision procedure for the current data predicate. The first obligation takes the form of an equality between the original data \( a \) and some unknown existential variable: \( a = ?_a \). The finishing tactic tries to solve this goal by using the equations built up in the data predicate during the correctness proof to rewrite the original encoded datatype into a term built entirely from parsed data, before unifying the resulting term with the \( ?_a \). Since \( a \) is not in the scope of the \( ?_a \), this latter step only succeeds when the rewritten term only depends on parsed data. The second obligation also uses an existential variable, this time to represent the decision procedure for the data predicate: \( P_A \text{dec'} \leftrightarrow ? \text{dec'} = \text{true} \). The tactic tries to discharge this goal by composing known decision procedures for predicates in \( P_A \) and simplifying away any tautologies, including any predicates built up during the correctness proof.

**Decoder Optimization** The final phase of `synthesize_decoder` tries to further simplify the synthesized decoder by rewriting with the monad laws and removing any redundant tests in the decision procedure synthesized in the previous step.

5. Extending the Framework

An extension to **NARCISSUS** consists of four pieces: a format, a decoder function, a proof of a \( \leftarrow \text{rule relating the two, and automation for incorporating this rule into `synthesize_decoder`}. As an example, consider the format of the Internet Protocol (IP) checksum used in the IP headers, TCP packets, and UDP packets featured in our case studies. Figure 11 presents the first three pieces of this extension. Note that `encode_IPChecksum` is a higher-order format combinator in the spirit of `ThenC`; the key difference is that it uses the bytestrings produced by the two format parameters to build the IP checksum (the one’s complement of the bytestrings interpreted as lists of bytes), which it then inserts between the two encoded bytestrings in the output bytestring. `decode_IPChecksum` first validates the checksum before decoding the rest of the string; the \( \leftarrow \text{rule for this decoder guarantees this test will always succeed for uncorrupted data, and can safely avoid parsing the rest of the string otherwise.}
TCP packets require adding the additional combinators to the framework noted in Figure 10 but do not require modifications to the core set of definitions. The source code for these parsers is included in the accompanying supplementary material.

The decoders that our framework produces are reasonably efficient and sufficiently full-featured to be used as a drop-in replacements for all parsing components of a typical TCP/IP stack. We support this claim by extracting our decoders to OCaml and integrating the resulting code into the pure-OCaml TCP/IP stack of MirageOS.

MirageOS [12] is a “library operating system that constructs unikernels for secure, high-performance network applications”: a collection of OCaml libraries that can be assembled into a stand-alone kernel running on top of the Xen hypervisor. Security is a core feature of MirageOS, making it a natural target to integrate our decoders into. Concretely, this entails patching the mirage-tcip library to replace its packet deserializers by our own verified decoders and evaluating the performance and functionality of the resulting library. This allowed us to benchmark a realistic network application, the mirage.io website (mirage-ww), off a networking stack enhanced with verified decoders. This shows that the overhead of using our decoders in real-life applications is very small.

---

1 https://github.com/mirage/mirage-tcip
2 https://github.com/mirage/mirage-ww

Figure 11. Binary format, decoder, and correctness rule for IP Checksums.

Figure 12. Format for IP version 4, utilizing the IP Checksum format.

The correctness rule for decode_IPChecksum, IPCORRECT, closely mirrors COMPOSECORRECT, adding additional assumptions that the bytestrings produced by each subformat have constant length and are properly byte-aligned; these assumptions are needed to prove the validity of the initial checksum test. Integrating this combinato into synthesize_decoder requires adding a new rule to the main loop of the tactic, keyon the encode_IPChecksum combinator. After applying IPCORRECT, this rule attempts to discharge the assumptions by rewriting with a database of facts about the lengths of encoded datatypes and the modulus operator, relying on the body of the main loop to synthesize decoders for the sub-formats. Figure 12 presents an example of the checksum combinator being used in the format for the IP headers.

6. Evaluation

To evaluate the expressiveness of NARCISSSUS, we implemented parsers for the set of network stack protocols shown in Figure 13. We note that the specifications of these formats are relatively short, consisting of on average roughly 180 lines of code. The specifications for DNS, IP, UDP, and
By themselves, our decoders are about fifty times slower than Mirage’s built-in decoders. The comparison is not entirely fair, however: we do significantly more validation (including checksum computations that require re-encoding a pseudoheader after decoding a TCP or UDP packet, where Mirage simply reads a few fields from an in-memory buffer), we rely on intermediate structures to ease integration with Mirage, and some parts of our framework are simply not heavily optimized (for example, our decoders fetch data bit-by-bit from the underlying data buffers; we could instead fetch whole bytes when the decoder performs byte-aligned reads).

**Set up** Starting with the derived encoders, we use Coq’s extraction mechanism to obtain OCaml libraries compatible with Mirage (extraction is mostly straightforward, though we customize it to use OCaml’s Int64 type for machine words, regular OCaml integers for numbers, and an efficient custom-built bit-string library to represent the bit buffers used for encoding and decoding). We then replace the TCP, UDP, IPv4, ARPV4, and Ethernet unmarshalling modules of the Mirage library with simple wrappers around our own extracted code and recompile the library and the Mirage website (patches against Mirage’s public repository¹ and setup instructions are included as supplementary materials). This whole process went very smoothly: Mirage’s test suite did not reveal issues with our decoders (we did have to adjust two tests: one of them used an IP packet with an EtherType that we do not support, and the other one unmarshalled a packet with an incorrect checksum, causing our decoders to reject it).

**Mirage’s website** We recompile the Mirage website to serve mirage.io atop a full user-space TCP/IP stack and measure page load times as we replace each decoder in the stack by its verified counterpart. We focus on the “blog” page of the website: loading it causes the client to fetch about 4 MB of data, obtained through 36 HTTP requests spread across 1040 TCP packets (covering page content, images, scripts, and stylesheets). We used the debugging API of the Chromium browser to accurately measure page load time. Figure 14 shows the average page load time across ten page loads: overall, transitioning all decoding to Fiat incurs a 7% page load overhead.

¹https://github.com/mirage/mirage

---

**7. Related Work**

**Existing Frameworks** There exist a number of frameworks for generating parsers and encoders. Traditional parser generators like YACC (Yet Another Compiler-Compiler) [10] and ANTLR [16] automatically generate parser implementations from declarative Backus–Naur form specifications. These frameworks decode inputs into the abstract syntax tree (AST) defined by the input grammar; users must post-process this AST (possibly using semantic actions) to convert it into the desired representation. Semantic actions are effectively user-defined programs that can easily introduce errors into the synthesized decoder.

An alternative approach is taken by interface generators like XDR [19], ASN.1 [7], Apache Avro [1], and Protocol Buffers [21], which generate encoders and decoders from user-defined data schemes. The underlying data format is defined by the system, however, preventing data exchange between programs using different frameworks. More importantly, the lack of fine-grained control over the physical data representation prevents users from extending the format in anyway, disallowing the use of interface generators with standardized formats like those used by network protocols.

The binpac compiler [15] supports a data-format specification language specifically developed for network protocols, including various general-purpose language constructs. Although binpac generates efficient protocol parsers for existing network protocols, this is no support for extending the specification language outside of the built-in constructs, and the system provides no formal guarantees about the generated code. More recent frameworks, like PADS [8], Packet-Types [13], and Datascript [2], feature sophisticated data-description languages with support for complex data dependencies and constraints for specific data schemes. Extending these frameworks with new encoding strategies requires directly modifying each system’s code generator, again with no guarantees about the correctness of the extended system.

Nail [4] is a tool for synthesizing parsers and generators from a high-level format. Nail unifies the data-description format and internal data layout into a single specification and allows users to specify and automatically check dependencies between encoded fields. More importantly, Nail natively supports extensions to its parsers and generators via user-defined stream transformations on the encoded data, allowing it to capture protocol features that other frameworks cannot. However, Nail provides no formal guarantees, and these transformations can introduce bugs violating the framework’s safety properties. We also note two other differences between Nail and NARCISSUS. First, Nail has many more orthogonal primitives than NARCISSUS has, as our primitives may be considered to be little more than the definition of decoder correctness. Second, while Nail provides flexibility in describing binary formats, it maps each format to a fixed C struct type, where NARCISSUS is compatible with arbitrary Coq types.
In contrast to these other frameworks, NARCISSUS provides a strong, machine-checked guarantee that every synthesized decoder properly inverts the data format and detects any malformed inputs. Using Coq’s logic as the specification language allows NARCISSUS to have a small trusted core of built-in features while still being both highly extensible and sound.

**Nondeterminism Monad** The nondeterminism monad [3] has a long history as a vehicle for deriving correct-by-construction programs by iterative refinement [6]. Recently, frameworks supporting this approach to program derivation have been developed for both the Coq [5] and Isabelle [11] proof assistants, with both systems providing machine-checked refinement proofs for derived software. While NARCISSUS does support the derivation of correct encoders via refinement of the nondeterministic function specifying a format, its approach to decoder synthesis does not. Rather, NARCISSUS builds the inversion of this relation specified by a format, ensuring that a synthesized decoder is sound with respect to every possible encoder function.

### 8. Future Work and Conclusion

We can imagine extending the library of NARCISSUS with several additional components. One natural set of additions would be compression schemes, allowing users to derive decoders for both archive formats like ZIP and image formats like PNG. The nondeterminism monad used in NARCISSUS specifications also provides a natural way to state nondeterministic perturbations to encoded data, allowing us potentially to characterize the resiliency of decoders to transmission errors; extending the library with components for error-correcting codes is another promising direction. Another future direction we plan to explore is integrating NARCISSUS-derived decoders and encoders into the development of certified Internet servers, like DNS and SMTP servers, and integrating the NARCISSUS-derived proofs to build strong end-to-end functional correctness guarantees. We would also like to improve the performance of encoders and decoders by pushing the derivation process further, to low-level imperative rather than just pure-functional code.

In conclusion, we have presented NARCISSUS, a framework for specifying and synthesizing correct-by-construction decoders and encoders from formats. This framework provides fine-grained control over the shape of encoded data, is extensible with user-defined formats and implementation strategies, has a small set of core definitions augmented with a library of common formats, and produces machine-checked proofs of soundness for derived decoders. We evaluated the expressiveness of NARCISSUS by deriving decoders for several standard networking protocols and evaluated the performance of the synthesized code by incorporating it into the networking stack of MirageOS.

### References


