Abstract
String-manipulating programs are an important class of programs with applications in malware detection, graphics, input sanitization for Web security, and large-scale HTML processing. This paper extends prior work on BEK, an expressive domain-specific language for writing string-manipulating programs, with algorithmic insights that make BEK both analyzable and data-parallel. By analyzable we mean that unlike most general purpose programming languages, many algebraic properties of a BEK program are decidable (i.e., one can check whether two programs commute or compute the inverse of a program). By data-parallel we mean that a BEK program can compute on arbitrary subsections of its input in parallel, thus exploiting parallel hardware. This latter requirement is particularly important for programs which operate on large data: without data parallelism, a programmer cannot hide the latency of reading data from various storage media (i.e., reading a terabyte of data from a modern hard drive takes about 3 hours). With a data-parallel approach, the system can split data across multiple disks and thus hide the latency of reading the data.

A BEK program is expressive: a programmer can use conditions, switch statements, and registers—or local variables—in order to implement common string-manipulating programs. Unfortunately, this expressivity induces data dependencies, which are an obstacle to parallelism. The key contribution of this paper is an algorithm which automatically removes these data dependencies by mapping a BEK program into a intermediate format consisting of symbolic transducers, which extend classical transducers with symbolic predicates and symbolic assignments. We present a novel algorithm that we call exploration which performs symbolic loop unrolling of these transducers to obtain simplified versions of the original program. We show how these simplified versions can then be lifted to a stateless form, and from there compiled to data-parallel hardware.

To evaluate the efficacy of our approach, we demonstrate up to 8x speedups for a number of real-world, BEK programs, (e.g., HTML encoder and decoder) on data-parallel hardware. To the best of our knowledge, these are the first data parallel implementation of these programs. To validate that our approach is correct, we use an automatic testing technique to compare our generated code to the original implementations and find no semantic deviations.

Categories and Subject Descriptors D.3.1 [Formal Definitions and Theory]: Semantics; D.3.2 [Language Classifications]: Specialized application languages; F.1.1 [Models of Computation]: Automata; F.4.3 [Formal Languages]: Decision problems

Keywords Symbolic Automaton; Symbolic Transducer; Satisfiability Modulo Theories; Data-Parallel; State Space Exploration

1. Introduction
BEK is a popular DSL for string-manipulating programs [15]. Because of its expressiveness and popularity, we have chosen to use it for our experiments. While much of our results can be applied broadly to symbolic finite-state transducers, our focus is on providing correct and performant implementations of symbolic finite-state transducers; BEK gives us a platform for doing so. The reader can browse some BEK programs online at http://rise4fun.com/Bek or read the BEK tutorial [23] to build his or her intuition. Typical BEK programs are string encoders and decoders, security sanitizers, etc.

Why BEK: The advantage of a domain-specific language is that, unlike most general-purpose languages, many algebraic properties are decidable for basic BEK (BEK programs that do not use registers). In particular, one can check whether such BEK programs commute or are idempotent; one can compute the inverse of a BEK program, and given an output, compute all inputs that lead to it.

While previous work has focused on algorithms for reasoning about basic BEK programs [15, 32], they did not provide a clear strategy for either running BEK on a variety of platforms, thus hindering its adoption, or providing algorithms that first transform BEK programs to their basic analyzable form. These are important problems as BEK programs are useful tools that developers use to secure both client-side web browsers and Internet scale web services. The goal of this paper is to demonstrate how to compile a BEK program to their basic form. Then, as a concrete application we show how to compile BEK programs into scalable data-parallel code.

Previous work has shown that special state variables, called registers in BEK, are often needed to express common functionality (Section 3). Unfortunately registers introduce data dependencies that are obstacles to parallelism and also make many forms of BEK analysis undecidable. Manually removing registers requires developers to reason about complex state, which is error-prone and time-consuming.

Exploration: A key contribution of this work is a novel exploration algorithm that is a form of loop unrolling combined with symbolic function composition. Loops are unrolled symbolically while data dependencies exist between consecutive iterations. Such unrolling is achieved by introducing new states for finite projections of registers. In this process, several characters may be grouped together into tokens by folding some part of a register symbolically into labels, while another part is folded into concrete states. Intuitively,
grouping changes the granularity of what is to be considered as a single input element. For example, if we take a program such as a UTF8 decoder, then grouping would create tokens that correspond to subsequences between 1 and 4 bytes,\(^1\) while for a BASE64 decoder it would create subsequences of fixed length 4.

While the algorithm is not guaranteed to work in all cases because it is undecidable, e.g. it is easy to encode reachability of two counter machines which is undecidable [16], when it does work, it produces a transducer that is behaviorally equivalent to the original up to grouping of the input sequence, but without register variables. We have not found any typical BFK programs, such as sanitizers, encoders or decoders, for which the technique would fail to terminate. A case when it does not work is a loop that for example counts the number of elements in the input or, in general, has arbitrarily long dependencies between input elements.

**Data parallelism:** There are two key benefits to a BFK program after exploration. First, registers induce data dependencies which limit parallelism and thus exploration is a necessary first step in exploiting parallelism. Second, after exploration, by construction, a BFK program has little intermediate state (e.g., complexity of a program is pushed to the edges rather than encoded as states). The overhead of our data parallel implementation of a BFK program is linearly related to the size of the BFK program’s intermediate state and thus exploration enables the automatic transformation from an expressive BFK program, with registers, into a data parallel one. This ultimately relieves the programmer from the burden of explicitly describing parallelism in a BFK program, an error-prone and difficult task.

### 1.1 Contributions

This paper makes the following contributions.

- Previous work on BFK introduced an extension to symbolic transducers with registers [32]. Use of registers is essential for modeling real sanitizers but makes their analysis difficult. In this paper, we present a novel exploration algorithm that is a form of symbolic loop unrolling that works modulo arbitrary decidable background theories. The algorithm terminates for a class of transduces that only need a bounded lookaheads and the algorithm outputs a new transducer that is equivalent to the input transducer but does not need registers.

- We integrated the exploration algorithm into a BFK to symbolic finite transducer (SFT) compiler. It has several interesting features. First, it uses an SMT solver as an oracle during the exploration algorithm, both for satisfiability checking and for model (witness) generation. Second, it combines exploration with grouping. Third, it uses the simplification mechanism present in modern SMT solvers for code generation of conditions and update functions.

- We demonstrate how exploration enables data parallelism. In particular, we show how to encode a BFK program, with infinite alphabets and registers, into one with a finite set of equivalence classes and no registers. Further, we demonstrate a data parallel implementation of this registerless intermediate form based on recent work in parallel finite state machines[25]. To the best of our knowledge, this is the first fully-automatic parallelization of string-manipulating code that combines advanced automata theory with state-of-the-art SMT technology to produce a parallel implementation.

- We have experimented with a number of BFK programs. We frequently observed exponential reductions in the number of states due to the application of our exploration algorithm. To validate the correctness of our translation, we used random testing of thousands of strings, observing no semantic differences when compared to independent C# serial implementations. For the range of hardware configurations we have experimented with, we observe a near-linear speedups as significant as 8x.

The background theories that were relevant for us during this work, were theories over linear arithmetic, bit-vectors, tuples, and lists. These theories were used to represent characters, tokens and strings. However, there were no dependencies on these particular theories. For example, one could also consider reals, rationals and arrays. Pragmatically speaking, any theory, or combination of theories, that is supported by an SMT solver works.

### 2. Background and Motivation

**String-manipulating programs:** Much of the practical motivation for analyzing string-manipulating routines comes from the need to analyze security sanitizers [15], such as the one shown in Figure 1. These are key in protecting against cross site scripting (“XSS”) attacks, which plague today’s web applications. These attacks happen because the applications take data from untrusted users, and then echo this data to other users of the application. Because web pages mix markup and JavaScript, this data may be interpreted as code by a browser, leading to arbitrary code execution with the privileges of the victim.

The first line of defense against XSS is the practice of sanitization, where untrusted data is passed through a sanitizer, a function that escapes or removes potentially dangerous strings. Multiple widely used Web frameworks offer sanitizer functions in libraries, and developers often add additional custom sanitizers due to performance or functionality constraints.

Sanitizers are typically a small amount of code, perhaps tens of lines. Furthermore, application developers know when they are writing a new, custom sanitizer or set of sanitizers. Experience has shown that if developers are willing to spend a little more time on sanitizers, they can obtain fast and precise analyses of sanitizer behavior, along with actual sanitizer code ready to be integrated into both server- and client-side applications. Our approach here is BFK, a language for modeling string transformations. The language is designed to be (a) sufficiently expressive to model real-world code, and (b) sufficiently restricted to allow fast, precise analysis, without needing to approximate the behavior of the code.

Unfortunately, implementing sanitizers correctly is surprisingly difficult. Anecdotally, in dozens of code reviews performed across various industries, just about any custom-written sanitizer was

---

\(^1\) Assuming standard Unicode text processing where code points are limited to 10FFFF in which case 4 bytes are enough, otherwise longer encodings up to 6 bytes are possible.
flawed with respect to security. SANER, for example, shows flaws in custom-written sanitizers used by ten web applications [2]. Incorrect sanitization may be worse than no sanitization by enabling rather than disabling JavaScript execution [4, 21].

The problem becomes even more complicated when considering that a web application may compose multiple sanitizers in the course of creating a web page. In a recent empirical analysis, it has been found that a large web application often applied the same sanitizers twice, despite these sanitizers not being idempotent [29]. This analysis also found that the order of applying different sanitizers could vary, leading to questions about whether composition of sanitizers is commutative.

BEK has been previously used to perform security-specific analyses of sanitizers. For example, one can use BEK to determine whether there exists an input to a sanitizer that yields any member of a publicly available database of strings [27] (XSS Cheat Sheet) known to result in cross site scripting attacks. Our analysis is fast in practice; for example, we take two seconds to check the commutativity of the entire set of Internet Explorer 8 XSS filters, and less than 39 seconds to check an implementation of the HTMLEncode sanitization function against target strings from the XSS Cheat Sheet [15].

Beyond strings: BEK has been demonstrated as being useful for applications beyond security sanitization. Other uses have been proposed, as diverse as image blurring and geo-location privacy, which fall outside the scope of this paper. The interested reader can see [32] for more details.

Performance: To realize why performance is a concern in this context, consider large-scale distributed data processing in the cloud. Encoding is paramount in Web applications, especially with large volumes of data. Google Docs or Office Web Apps, for example, store multi-megabyte files from millions of users. XSS caused by insufficient data sanitization has been discovered in these large-scale cloud apps before. To avoid XSS, these services must encode all user files before displaying them on the web.

3. Symbolic Transducers

The semantics of BEK programs are given by symbolic transducers. The goal of this section is to recap the BEK language in Section 3.1. In Section 3.2, we develop a formal treatment required to precisely express these semantics. Pragmatically-inclined readers may wish to save Section 3.2 for later reading.

3.1 Intuition

We briefly describe the BEK domain-specific language for writing string transformations such as shown in Figure 1. An example BEK program is in Figure 2. As introduced in [15], the core construct in BEK is iteration over each character in an input string. Programs can then have case statements that describe different behavior for different input characters. Typically the program will perform some local computation, then yield, or output, a new character. A new string is built up based on the characters of the input string.

Registers: Programs can also have register variables that keep state during the iteration. Figure 2 shows a sample BEK program that checks each character and then updates a register variable r. Depending on input character, the program may then output the contents of the register, or it may simply pass through the character unchanged. An end case statement takes care of any remaining final output suffix after the end of the input has been reached. For more details on BEK we refer to previous work or to the online BEK evaluator [23]. While the language is limited, it still is expressive enough to capture a wide range of string-manipulating functions, including many of the functions commonly used in Web sanitization and functions used in graphics processing [15, 32].

ST Representation: The semantics of the program in Figure 2 is captured by a symbolic transducer in Figure 3. Symbolic transducers are a generalization of classic finite transducers, which allow arbitrary underlying label theories [32].

Exploration and Data-Parallelism: The register variables in BEK are important for making it easy to translate string-manipulating functions written in C# or other languages to BEK, because existing functions typically keep state through an iteration. These variables are also convenient for writing functions in BEK directly. Unfortunately, these register variables are enemies of data-parallelism, because they introduce control flow that depends on the registers and not on the individual character.

3.2 Formalism

We now formally define symbolic transducers or STs and give examples of how STs capture behavior of programs. We assume a background structure that has an effectively enumerable background universe U, and is equipped with a language of function and relation symbols with fixed interpretations. Definitions below are given with U as an implicit parameter. We assume closure under Boolean operations and equality. Operations that are specific to U do not affect the results. We use λ-expressions for dealing with
anonymous functions that we call \( \lambda \)-terms. In general, we use standard first-order logic and follow the notational conventions that are consistent with [32]. The universe is multi-typed with \( \tau \) denoting the subuniverse of elements of type \( \tau \). We make use of the empty tuple type \( T_0 \) such that \( T_0 = \{ () \} \). We use a variant of the definition of STs where the control state component of STs is explicit. We write \( \Psi(\sigma) \) for the set of \( \sigma \)-predicates. We write \( \Lambda(\sigma \rightarrow q) \) for \( \lambda \)-terms \( f \) that denote functions \( f : \sigma \rightarrow \gamma \). We write \( \Lambda(\sigma \rightarrow q)^+ \) for \( \bigcup_{\sigma} \Lambda(\sigma \rightarrow q^+) \). In other words, for any \( \lambda \)-term \( f \in \Lambda(\sigma \rightarrow q)^+ \) the length of the output sequence may not depend on the input, but must be fixed.

**Definition 2**: A Symbolic Transducer or ST with input type \( \tau \) and output type \( \gamma \) and register type \( \tau \) is a tuple \( A = (Q, q_0, \tau, R) \), where \( Q \) is a finite set of states; \( q_0 \) is the initial state; \( \tau \) is the initial register value; \( R \) is a finite set of rules \( R = \Delta \cup F \) where \( \Delta \subseteq (Q \times (\sigma \times \tau) \times \Lambda(\sigma \rightarrow q)^+) \times \Lambda(\tau \rightarrow \gamma) \) is a set of transitions and \( F \subseteq (Q \times \Psi(\tau) \times \Lambda(\tau \rightarrow \gamma)) \) is a set of finalizers.

A transition \( (q, \varphi, \sigma, u, \rho) \) is also written \( q \xrightarrow{\varphi/o,u} \rho \) where \( q \) is the start state, \( \varphi \) the guard, \( \sigma \) the output, \( u \) the update, and \( \rho \) the end state. A finalizer \( (q, \varphi, \sigma) \) is also written \( q \xrightarrow{\varphi/o} \sigma \) with \( q \) as the state, \( \varphi \) as the guard, \( \sigma \) as the output. Finalizers generalize final states.

**Example 1** Let \( \sigma = \gamma \) be unsigned bitvectors (or natural numbers) \( N \) and let \( \tau \) be the type \( \mathbb{N} \times \mathbb{N} \). The operation ‘\( \ll \)’ is shift-left, ‘\( \gg \)’ is shift-right, ‘\( \& \)’ is bit-wise-AND, ‘\( \| \)’ is bit-wise-OR. The ST in Figure 3 has the above types and is the direct mapping of the BEK program in Figure 2 where \( s = y[1] \) and \( r = y[2] \). \( Q = \{ q \} \), \( r^0 = (0, 0) \), and the ST has two transitions and three finalizers. It computes Base64 encoding of byte sequences. Base64 is a standard encoding that is used to transfer binary data over textual media.

The semantics of \( A \) is given by the following concrete transition relation.

Let \( q,p,q' \in Q \), \( r \in \tau \), \( \sigma \in \alpha \). Then \( (q,r) \xrightarrow{\sigma/o,u} A \) \((p,u(a,r)) \) denotes that there exists a transition \( q \xrightarrow{\varphi/o,u} \rho \) such that \( \varphi(a,r) \) holds. Similarly, \( (q,r) \xrightarrow{\sigma/o} A \) \( \otimes \) denotes that there exists a finalizer \( q \xrightarrow{\varphi/o} \sigma \) such that \( \varphi(r) \) holds.

Now, the reachability relation \( p \xrightarrow{\sigma/o} A \) \( p' \) for \( \sigma \in \sigma^* \), \( \delta \in \gamma^* \), and \( p' \in \{ Q \times \tau \} \cup \{ \emptyset \} \) is defined through the closure under the following conditions, where ‘\( \gamma \)’ is concatenation of sequences, note that \( \epsilon = \bar{x} = \bar{x} = \bar{x} = \bar{x} \):

- If \( p \xrightarrow{\sigma/o} A \) \( p' \) then \( p \xrightarrow{\sigma/o} A \) \( p' \).
- If \( p \xrightarrow{\sigma/o} A \) \( p' \) then \( p \xrightarrow{\sigma/o} A \) \( p' \).

**Definition 2**: The transduction of \( A \), denoted \( \mathcal{B}_A \), is the following function from \( \sigma^* \) to \( 2(\gamma^*)^* \):

\[
\mathcal{B}_A(\bar{a}) \triangleq [\bar{b}] (q^0_t, r^0_t) \xrightarrow{a/b} A \otimes \)

\( A \) is single-valued when \( |\mathcal{B}_A(\bar{a})| \leq 1 \) for all \( \bar{a} \in (\sigma)^* \) and \( A \) is deterministic when, for all \( \bar{a}, \bar{b}, \bar{b}', p, p_1, p_2 \), if \( p \xrightarrow{a/b} A \) \( p_1 \) and \( p \xrightarrow{a/b} A \) \( p_2 \) then \( b_1 = b_2 \) and \( p_1 = p_2 \). We write \( \mathcal{B}_A(\bar{a}, \bar{b}) \) for \( \bar{b} \in \mathcal{B}_A(\bar{a}) \).

Finalizers can be omitted at the expense of allowing nondeterminism. However, nondeterminism is undesired because determination of STs is in general not possible and analysis of (or even code generation from) nondeterministic STs is very difficult.

It is easy to show that determinism implies single-valuedness. Deterministic STs form a practically important subclass of STs and in the examples and case studies we only consider deterministic STs. For the data-parallel translation explained in Section 5 the STs are required to be deterministic, that is naturally the case for the kinds of string transformations we have in mind with this approach.

**Example 2** Let \( A \) be the ST in Figure 3. Let \( y = \langle 0, 0 \rangle \) and \( x = \langle a' \rangle = 1000001 \). So \( x \leq 255 \) and \( y[1] \neq 2. \) We have \( E(x \gg 2) = E(100002) = E(16) = 16 + 65 = \langle q' \rangle \) and \( (x \& 3) \& 4 = \langle 1 \& 4 \rangle = 100002 = 16 \), so there is a concrete transition

\( (q, 0, 0) \xrightarrow{\langle a' \rangle} (q, 1, 16) \)

If we do one more step from configuration \( (q, \langle 1, 16 \rangle) \) with input \( \langle b \rangle \) we get the concrete transition

\( (q, \langle 1, 16 \rangle) \xrightarrow{\langle b \rangle} (q, 2, 8) \)

Suppose that the input sequence ends here. Then we use the last finalizer that gives us the concrete transition:

\( (q, 2, 8) \xrightarrow{\langle 11 \rangle} \)

By using the derived reachability relation we have

\( (q, 0, 0) \xrightarrow{\langle a' \rangle, \langle b \rangle} (q, \langle 1, 16 \rangle) \)

Thus, \( \mathcal{B}_A(\langle AB \rangle) = \langle \lbrace QU^* \rangle \rangle \).

**4. Compilation of STs to SFTs**

We assume that an ST is given. The ST may for example be the result of a translation from a BEK program. Sample BEK program and corresponding ST are illustrated in Figure 2 and Figure 3. Our goal is to compile the ST into an SFT (if possible), where an SFT is an ST without registers, or formally, whose register type \( \tau \) is \( T_0 \). In the SFT we may group some characters into combined characters or tokens so that, if the input type of the ST is \( \sigma \) then the input type of the SFT is \( \sigma^* \) for some \( k \geq 1 \) (sequences over \( \sigma \) of length \( l \leq k \)). In our compilation we maintain the following equivalence between the given ST and the resulting SFT. We use \( \text{flatten}[\langle u_i \rangle_{i=1}^\sigma] \), where \( u_i \) has type \( \sigma^* \), to denote the sequence \( u_1 \cdot u_2 \cdot \ldots \cdot u_n \) in \( \sigma^* \).

**Definition 3**: ST and SFT are equivalent modulo grouping if \( \forall a, b \), \( \mathcal{B}_A(a, b) \iff \exists u_i : a = \text{flatten}(\langle \bar{a} \rangle), \mathcal{B}_A(\bar{a}, \bar{b}) \).

In other words, the outputs of ST and SFT must be equal for some grouping of the input characters in SFT. The compiler uses two phases, grouping and exploration. The phases are interleaved into a single algorithm, but intuitively, they serve two distinct purposes:

**Grouping**: The idea is as follows. Two consecutive transitions \( p \xrightarrow{\varphi/o,u} q \xrightarrow{\varphi'/o,u'} q' \) can be lifted into a single transition that reads more inputs in one atomic step

\[
\lambda(x,y), \varphi(x[1], y) \wedge \varphi'(x[2], u(x[1], y)) / \\
\lambda(x,y), o(x[1], y) \wedge o'(x[2], u(x[1], y)) / \\
\lambda(x,y), u'(x[2], u(x[1], y)) \rightarrow q
\]

where \( x[i] \) reads the \( i \)-th element from \( x \) (suppose first element has index 1). Thereby, the state \( q' \) becomes eliminated (if this is the only occurrence of \( q' \)). The lifted transition may also become unsatisfiable, in which case it is eliminated. The input character of the new transition is a pair of the original characters.

**Exploration**: Exploration starts from the initial configuration \( \langle q', r' \rangle \) where \( q' \) is the initial state and \( r' \) is the initial register value of the ST. If an update to a register is a fixed value \( r \) that is independent of the input values in a given target state \( q \) of the ST, then the configuration \( (q, r) \) is treated as a state
def _init_(self, q0, r0, T, F, x, y, ax):
    self.q0 = q0  # initial state
    self.r0 = r0  # initial register
    self.T = T  # transitions
    self.F = F  # finalizers
    self.x = x  # label variable
    self.y = y  # register variable
    self.ax = ax  # background axioms

def Delta(self, q):
    # transitions from q
    for t in self.T:
        if t[0] == q:
            yield t

def Fin(self, q):
    # finalizers from q
    for t in self.F:
        if t[0] == q:
            yield t

def GetUniqueValue(st, phi, t, k):
    x = lambda i: Const('x%d' % i, st.x.sort())
    z = lambda i: Const('z%d' % i, st.x.sort())
    theta = { [x(i), z(i)] for i in range(k) }
    t1 = substitute(t, theta)
    phi = substitute(phi, theta)
    if st.IsSat(And(phi, t1)): return None
    else: return GetUniqueValue(st, phi, t+1)

def Explore(st):
    Z.add(axioms)
    def Explore(st):
        W, sft = {}, []
        for stateMap in st.stateMap:
            for state in stateMap:
                yield stateMap[state]
The third point is: The reason we are interested in SFTs. The second point is: When does the exploration algorithm terminate? The third point is: Does the algorithm meet our needs for parallelization? As it turns out, the third question needs more work – because, except for some special cases when the lookahead is fixed, the assumption that the input is tokenized up front is not true. The reason we are interested in SFTs.

4.1 Succinctness

Figure 6. SFT after grouping of ST in Figure 5; \( y^m \) denotes extraction of bits from \( m \) to \( n \) from \( y \); \( y \cdot z \) denotes bit-append.

comes independent of the register \( r \) because \( r \) is only used to glue \( f \) with \( g \) and \( q \).

A similar step is applied to transitions followed by finalizers to get composed transitions that lead from \( p_0 \) to sink states \( p_1 \) and \( p_2 \) (states without outgoing transitions and with trivial finalizers that yield empty outputs). Finally, all resulting rules are independent of the register and so the register can be eliminated and we have constructed an SFT illustrated in Figure 6. An important point is that the construction of the SFT would not be possible by only using grouping or only using naive exploration. The new combined exploration algorithm is needed.

The first point we address next is: The reason we are interested in SFTs. The second point is: When does the exploration algorithm terminate? The third point is: Does the algorithm meet our needs for parallelization? As it turns out, the third question needs more work – because, except for some special cases when the lookahead is fixed, the assumption that the input is tokenized up front is not true. The reason we are interested in SFTs.

4.1 Succinctness

Figure 7 compares the sizes of the state machines needed to achieve the different encoding and decoding tasks.

<table>
<thead>
<tr>
<th>Encoder</th>
<th>Size</th>
</tr>
</thead>
<tbody>
<tr>
<td>UTF8encode</td>
<td>6</td>
</tr>
<tr>
<td>UTF8decode</td>
<td>10</td>
</tr>
<tr>
<td>BASE64encode</td>
<td>105</td>
</tr>
<tr>
<td>BASE64decode</td>
<td>1161</td>
</tr>
<tr>
<td>HTMLencode</td>
<td>33</td>
</tr>
<tr>
<td>HTMLdecimal</td>
<td>113</td>
</tr>
</tbody>
</table>

Figure 7. Exploration sizes in total nr of transitions. SFT is naive exploration. SFT+ is grouped exploration. k-SFT is creation of k-SFT after SFT+.

The table indicates the advantages of using the exploration algorithm. Without this dramatic reduction in the size of the SFT, we would not be able to compile the SFT to exploit data parallel finite state machines presented below, where the approach requires that the number of states in the transducer is small, which our compilation scheme provides, while the label theory may potentially allow infinite character domains. In particular, it is shown in [32, Figure 8(a)], that in HTML decoding, the number of states in the SFT grows exponentially in the length of \( k \) for supporting decoding of patterns \( k \# [0 \ldots 9] \{k\} \); that makes naive exploration to SFTs impractical in this case. This exponential blowup is avoided with the new exploration algorithm. The final column in the table shows the size of the k-SFT obtained after the final phase of the algorithm discussed below.

**Definition 4:** A k-SFT has a finite state space \( Q \) and has transitions \( p \xrightarrow{\iota} q \) where \( p, q \in Q \), \( \iota \) is a \( \sigma \)-predicate, and \( f \in \Lambda(\sigma^m \rightarrow n) \) is a \( \lambda \)-term for some fixed \( m \geq 0 \) and \( n \geq 0 \). We assume that the k-SFT is deterministic meaning that if there are two transitions \( p \xrightarrow{\phi_1/f_1} q_1 \) and \( p \xrightarrow{\phi_2/f_2} q_2 \) such that \( \phi_1 \land \phi_2 \) is satisfiable, then \( f_1 = f_2 \) and \( q_1 = q_2 \). A k-SFT has also finalizers of the form \( q \rightarrow \gamma \) with \( f \) as above and \( \gamma \) to maintain determinism there is at most one finalizer for each state \( q \). The case \( m = 0 \) means that there is no input dependence, so \( f \) is a fixed output sequence.

The semantics of a transition \( p \xrightarrow{\phi/f} q \) is that \( \phi \) is applied in state \( p \) to the current character in the input sequence \( \iota \), say \( \iota_l \). There is an implicit well-definedness criterion that, if the state is \( p \) and \( \phi(c_l) \) is true then \( i \leq m \), where \( m \) is the arity of \( \phi \). If \( \phi(c_l) \) holds then \( f \) is applied to \( (c_{i-m+1}, c_{i-m+2}, \ldots, c_{i-1}, c_i) \) to produce the suffix of the output. For finalizers the semantics is that \( f \) is applied to \( (c_{i-m+1}, c_{i-m+2}, \ldots, c_{i-1}, c_i) \) to produce the suffix of the output.

4.2 Termination and Limitations

The exploration algorithm does not terminate if there are unbounded dependencies between successive characters in the input. In other words, if the register is needed to remember some input element for arbitrarily many following input elements. For example, if the register is used to sum all “digits” seen in the input, then the exploration algorithm does not terminate.

An m-grouping of a nonempty sequence \( \bar{a} \) over \( \sigma \) is a sequence \( \bar{a} \) over \( \sigma^m \) whose flattened form equals \( a \). For example, the sequence \( [[1, 2], [3, 4, 5], [6]] \) is a 3-grouping of the sequence \([1, 2, 3, 4, 5, 6] \).

**Definition 5**: ST \( A \) has the bounded lookahead property if there is a finite subset \( P \subseteq Q \times \tau \), \( p_0 = (q^0, i^0) \in P \), and there exists \( m > 0 \) such that for all input sequences \( \bar{a} \) over \( \sigma \) accepted by \( A \) there exists an m-grouping \( [u_i]_{i=1}^{m+1} \) of \( \bar{a} \) such that \( p_{i-1} \xrightarrow{\iota_i} p_i \) for some \( p_i \in P \) for \( i < n \) and \( p_n = \emptyset \).

**Theorem 1**: Exploration algorithm terminates iff the ST has the bounded lookahead property. The output SFT is equivalent modulo grouping to the input ST.

We write SFT+ for the intermediate result that the exploration algorithm produces. Namely, SFT+ stands for the SFT whose input characters have been grouped, i.e., whose character type is \( \sigma^m \), for some \( m > 0 \), where \( \sigma \) is the character type of the input SFT.

There is a class of STs for which the exploration algorithm does not terminate although an equivalent k-SFT exists. Roughly speaking, this situation arises when bounded lookahead cannot be turned into bounded lookahead. Thus, even if the ST could, in principle, be compiled into an equivalent k-SFT, there exists no intermediate SFT+ over grouped characters.

The following example illustrates such a case.

**Example 4**: Consider standard \&#x21EA; code over full Unicode. An input to the encoder is a UTF-16 encoded string. An input is malformed if it contains a bad surrogate \( b \):

- \( b \) is a high surrogate in range \( \psi_{m_0}^{m_1} \leq \lambda x.55296 \leq x \leq 56319 \) that is not immediately followed by a low surrogate (range \( \psi_{m_0}^{m_1} \leq \lambda x.56320 \leq x \leq 57343 \)), or
- \( b \) is a low surrogate that is not immediately preceded by a high surrogate.
Some encoders use the following correcting rule as a robustness feature rather than rejecting malformed strings (e.g., `HtmlEncode` in `System.Net.WebUtility` in .NET Framework 4.5). The Unicode replacement character \(\uFFFD\) (uFFFD) is used to replace bad surrogates so that the string is not malformed. Such a correcting phase can be described by the ST in Figure 8(a), say \(\text{Rep}\). For efficiency, an equivalent \(k\)-SFT, say \(M\). Finally, \(M\) is composed with \(\text{Rep}\) (the 2-SFT in Figure 8(b)) to produce \(M' = \lambda x. M(\text{Rep}(x))\). Although \(k\)-SFTs are, in general, not closed under composition, in this particular case they are. So the actual input to parallelization is \(M'\). Not only is this easier to program, but it is also less error-prone because the corner cases of what to do with bad surrogates are completely avoided. Moreover, there is no loss in efficiency because the two transformations are automatically composed into one, essentially eliminating the intermediate corrected string, as a form of deforestation [34].

Example 4 illustrates a case when it is not possible to construct \(SFT^+\) from \(ST\) because there is no grouping bound, although an equivalent \(k\)-SFT exists. Another difficulty is that it is not always possible to turn an \(SFT^+\) into a \(k\)-SFT (that is required for parallelization unless all groups have a fixed length). As discussed below, such a transformation requires monadic decomposition of predicates [33] in order to decompose \(n\)-ary relations used as guards in the \(SFT^+\) into Boolean combinations of monadic relations that will guard the transitions in the \(k\)-SFT. In general this is not possible, e.g., if the predicate is \(x = y\). Moreover, the problem of deciding if such a decomposition exists is, in general, undecidable even when assuming (as we do) that the theory over labels is decidable. The latter undecidability follows from a result in [20, Proposition 2.b].

### 4.3 Parallelizability

The exploration algorithm presented above transforms an \(ST\) into an \(SFT\) at the expense of grouping several input characters into one token. Thus, formally the input language of the \(SFT\) is a nested sequence where the inner sequences or character groups are tokens. If all tokens have the same length \(k\), as in Base64 decoding where \(k = 4\), then it is possible to process the original input in parallel by reading the input tokens from offsets \(km\) for \(m > 0\). In general, as for example with HTML encoding or UTF8 encoding, the tokens have variable length and this simple solution does not work. Also, storing inputs in registers breaks parallelizability and takes us back to square one.

Instead, we transform the \(SFT^+\) into a \(k\)-SFT with lookback building on the idea of \(k\)-SLTs introduced in [7]. The algorithm that we use does not introduce registers and maintains the property that transition guards only reference the current character, but output functions may refer back to \(k\) prior input characters. The resulting \(k\)-SFT is a special kind of a \(k\)-SLT. The main benefit is that the transition graph of the domain of a \(k\)-SFT is an SFA over the original characters. This enables the parallelization approach presented in Section 5 and the output computation still works because the lookback is bounded and can be applied in parallel.

We illustrate the algorithm below using an example. The input to the algorithm is an \(SFT\) over tokens or subsequences of characters. This \(SFT\) is first decomposed so that all transitions are split into predicates over singleton characters. To achieve this, the algorithm uses monadic decomposition of predicates from [33]. Then the split transitions are merged back together into a deterministic \(k\)-SFT. Finally, the \(k\)-SFT is compiled into C# code that is used by the subsequent parallelization step.

**Example 5** We consider here a cut down version of a UTF8 decoder to illustrate \(k\)-SFT construction. Suppose that the \(SFT^+\) produced by exploration has a single state \(q_0\) and three transitions: \(q_0 \rightarrow q_0, q_1,\) and \(q_0 \rightarrow q_0\), where

- \(\psi\) reads one byte and checks that it is in the ASCII range and the character is output as is,
- \(\varphi\) reads two bytes and checks that they form a valid 2-byte encoding, \(f\) computes the code point from the two bytes,
add the numbers in two sequences we could use
\[
\text{zip}(\cdot, [0,1,2], [3,4,5]) = [3,5,7]
\]
Second, \text{scan} applies a binary \textit{associative function}, \(\oplus\), over every prefix of a sequence, i.e., given a sequence \([x_1, x_2, \ldots, x_n, x_{n+1}]\), and an identity element \(s\) such that \(s \oplus x = x\), \text{scan} produces
\[
[r, x_1, (x_1 \oplus x_2), (x_1 \oplus x_2 \oplus x_3), \ldots, (x_1 \oplus \cdots \oplus x_n)]
\]
For explanatory purposes we use a related function \text{scanf} that takes a function \(\odot : Q \times \sigma \rightarrow Q\), a value \(q_0 \in Q\), a sequence \([s_1, \ldots, s_n, s_{n+1}]\) \(\in \sigma^*\) and produces the sequence
\[
[q, q \odot s_1, ((q \odot s_1) \odot s_2), \ldots, (((q \odot s_1) \odot s_2) \odot \cdots \odot s_n)]
\]in \(Q^*\) of length \(n + 1\). Finally, we use the function \text{split} to split a given sequence \(s\) according to a sequence \(m\) of lookback offsets as follows into a sequence of tuples (or subsequences):
\[
\text{split}([s_1, \ldots, s_n]) = [(s_{i+1-m_i}, s_{i+2-m_i}, \ldots, s_{i})]_{i=1}^{n}
\]
We next show how to define SFTs in terms of these primitives.

5.2 Describing SFTs With Higher-Order Functions

Recall that a k-SFT \(M\) is a tuple \((Q, q_0, R)\) where \(q_0\) is the initial state, and \(R = \Delta \cup F\) is a finite set of rules, consisting of \textit{transitions} \(\Delta\) and \textit{finalizers} \(F\). Here we require \(M\) to be deterministic. Moreover, for ease of presentation and without loss of generality, we assume that all finalizers of \(M\) are trivial in the sense that they produce the empty output and are thus treated as final states in the classical sense. For example the 2-SFT in Figure 8(b) is deterministic. We assume that we work with an extended alphabet where there is an end-of-input (EOI) symbol and all valid input sequences end with EOI, so that finalizers are not needed. For each transition \(p \xrightarrow{f/q} q\) we refer to the arity of \(f\) as the \textit{lookback} of the transition, that is denoted by \(\ell(p,a)\) where \(a \in [\sigma]\). We represent normal characters by their code points as (negative) integers. EOI has code \(-1\). We refer to \(f\) by \(\phi(p,a)\), i.e., \(\phi(p,a)\) takes \(\ell(p,a)\) arguments.

Thus, the rules define a transition \textit{function} from a given input and state to an output and a new state. Let \(\delta(q,a)\) be the state \textit{function}, implicitly defined by the rule set \(R\), which takes as arguments a state \(q\) and an input \(a\) and produces a new state.

To transduce an input sequence \(s\), \(M\) starts in state \(q_1 = q_0\) and sequentially reads the symbols of \(s\). When \(M\) reads the \(i\)th symbol \(s_i\) from \(s\) in state \(q_i\) (first symbol being \(s_1\)), it enters state \(q_{i+1} = \delta(q_i,s_i)\) and calls the output function \(\phi(q_i,a)\), where \(a = [s_{i+1-m_i}, s_{i+2-m_i}, \ldots, s_i]\), which maps to a finite (possibly empty) sequence of symbols in the output alphabet. We call the algorithm to transduce a string by \(M\), \text{Transduce}, it takes as input \(M\) and a sequence \(s\) and produces the output sequence.

\[
\text{Transduce}(M, s) = \begin{align*}
&\text{let } q = \text{scanf}(\delta, q_0, s) \text{ in } \\
&\text{let } m = \text{zip}(\ell(q, s)) \text{ in } \\
&\text{flatten}(\text{zip}(\delta, q, \text{split}(s, m)))
\end{align*}
\]
where \text{flatten} is defined in Section 4.

Example 6 Consider the 2-SFT \(R_\text{ep}\) in Figure 8(b). We first extend \(R_\text{ep}\) so that it has the final state \(q_2\) and we assume that all valid inputs end with EOI. We write \(\hat{h}\) for \(\psi_H\). We write \(\mathcal{S}\) for \(\mathcal{L}_\lambda(x = EOI)\) and we write \(\mathcal{H}\) for \(\lambda x. \neg(x) \land \neg h(x)\). We also add a fourth state \(q_3\) that corresponds to an \textit{error state} (in practice this state may often be omitted, but we include it here for clarity). Let \(\text{flip} \equiv \text{flip}(\psi_L, x)\) then \(\#\) else \(x\) and let \(g \equiv \lambda (x_{-1}, x).[(\psi_L(x) \text{ then } x_{-1} \text{ else } \#), x]\). The extended 2-SFT is depicted in Figure 10. Let \(a = \text{D8}3\text{D16}\) and \(b = \text{DE0A16}\). So \(h(a)\) holds and \(\psi_L(b)\) (thus also \(h(b)\)) holds. Take the input

\[\begin{align*}
\text{zip}(+, [0,1,2], [3,4,5]) &= [3,5,7] \\
\text{split}([s_1, \ldots, s_n]) &= [(s_{i+1-m_i}, s_{i+2-m_i}, \ldots, s_i)]_{i=1}^{n}
\end{align*}\]
Graph Traversals with Matrix Multiplication: A convenient way to view k-SFT is as a graph where the nodes are states and there exists an edge from state \( i \) to state \( j \) on symbol \( s \) if \( \delta(i, s) = j \). A graph is simple to represent as an adjacency matrix: the set of traversal steps \( \delta \) is the equivalence class of states that are not connected by any edge. The \( \delta \) function represents the transition relation between states and symbols in the input alphabet. We compile \( \delta \) to an adjacency matrix \( M \), which can be effectively used by constructing all the satisfiable Boolean combinations over \( \Psi \), for this we use the minterm algorithm from [9].

Example 7 Consider the 2-SFT \( \text{Rep} \) in Figure 10. \( \text{Rep} \) uses four guards. The minterms are \([h, h, s]\) because they are all pairwise disjoints and their union equals \( T \). The SFA corresponding to \( \text{Rep} \) looks exactly the same as \( \text{Rep} \) but with output functions omitted. Since there are three equivalence classes, say \( A = [h], B = [s], \) and \( C = [s] \), we have three adjacency matrices \( (M_A, M_B, M_C) \) that describe how every state in the SFA transitions when reading symbols \( a \in A, b \in B \), and \( c \in C \), respectively.

\[
M_A = \begin{bmatrix}
0 & 1 & 0 & 0 \\
0 & 0 & 1 & 0 \\
0 & 0 & 0 & 1 \\
0 & 0 & 0 & 1
\end{bmatrix}, \quad M_B = \begin{bmatrix}
1 & 0 & 0 & 0 \\
0 & 1 & 0 & 0 \\
0 & 0 & 1 & 0 \\
0 & 0 & 0 & 1
\end{bmatrix}, \quad M_C = \begin{bmatrix}
0 & 0 & 1 & 0 \\
0 & 0 & 0 & 1 \\
0 & 0 & 0 & 1 \\
0 & 0 & 0 & 1
\end{bmatrix}
\]

Given \( a \) and \( b \) as in Example 6, we have \( a \in A \) and \( b \in B \).

Given this formulation, we use matrix multiplication \( \cdot \) as a mechanism for graph traversal. Assume the identity matrix \( I \) encodes the initial state of the SFA. Then adjacency matrix that encodes the state of the SFA after reading the first symbol \( a \) in an input sequence \( s \) is \( I \cdot M_a \). Further, the adjacency matrix that encodes the state of the SFA after reading the second symbol, \( b \) of \( s \) is \( I \cdot M_a \cdot M_b \), etc.

From k-SFTs to matrices: To transform a k-SFT to operations on vectors and matrices, we define the following two functions, \( \text{inflation} \) and \( \text{project}: \) \( \text{inflation} \) generates the matrix \( M_a \) for each symbol \( a \in \sigma \); \( \text{project} \) extracts from matrix \( M_w \) the state of the (underlying) SFA, where \( M_w \) is obtained after reading the input sequence \( w \), starting from state \( q_0 = 0 \):

\[
\text{project}(M_w) = V_0 \cdot M_w \cdot V_F
\]

where \( V_0 = (1, 0, \ldots, 0) \) and \( V_F \) is an \( n \)-component column vector

\[
V_F^T = (0, 1, \ldots, n - 1).
\]

So \( V_0 \cdot M_w \) extracts the first row, say \( X, \) of \( M_w \), where \( X \) has exactly one element \( j \) that is \( 1 \) while all the other elements are \( 0 \) because the SFA is deterministic, where \( j \) is the state reached from \( q_0 \) after reading \( w \). Thus \( X \cdot V_F \) is the state that \( j \).

Given this formulation, we implement an associative version of \( \delta \) of the transition function \( \delta \) that uses “inflated” symbols instead of actual symbols. Thus, instead of using the actual alphabet, the transduction uses the inflated alphabet \( \{M_a \mid a \in \sigma \} \) and the input sequence is mapped to the inflated alphabet through the initial inflation of the input sequence \( \text{map}(\text{inflation}; s) \):

\[
\tilde{\delta}(M_a, M_a) \iff M \cdot M_a
\]

where \( M \) is a matrix that encodes the state of the SFA, and \( M_a \) is the inflated symbol \( a \). Therefore, the function \( \tilde{\delta} \) is associative by associativity of matrix multiplication and enables us to implement a data parallel version of \( \text{Transduce} \) as:

\[
\text{Transduce}(k\text{-SFT}, s) \triangleq
dl q = \text{map}(\text{project}, \text{scan}(\tilde{\delta}, S)) \text{ in}
\text{let } m = \text{zip}(\ell, q, S) \text{ in}
\text{flatten}(\text{zip}(q, \delta, \text{split}(s, m)))
\]

An important point to note is that \( \phi \) must be applied to the original (non-inflated) sequence \( s \) because the output functions of the rules of the SFT depend on the actual input, while both \( \ell \) and \( \delta \) are lifted to work directly on the equivalence classes.

\[\text{Figure 10. 2-SFT Rep extended with EDI. The state } q_2 \text{ is the final state, meaning that it has the trivial finalizer } q_2 \xrightarrow{\circ}.\]
5.4 An Efficient Matrix Representation

While matrix multiplication is associative, it unfortunately has a high overhead. Even an optimized implementation requires a significant amount of computation and memory—matrix multiplication runs in $O(m^3)$ where $m$ is the number of states in a finite state automaton and requires $m^2$ memory.

To reduce this overhead such that it is linear in the number of states (both time and space), we exploit the fact that all of our adjacency matrices are square binary matrices with exactly one 1 in each row (and zeros elsewhere). We follow recent work and succinctly represent this type of adjacency matrix as an array where the value of the array at index $i$ (staring from 0) is equal to the index of the column that contains a 1 for row $i$ [25]. This is possible because each row contains exactly one 1.

In other words, the matrix is encoded as a one-dimensional array indexed by states. For example, the matrices $M_A$ and $M_B$ from the prior section, represented as arrays are $[1, 1, 3, 3]$ and $[0, 0, 3, 3]$, respectively. With this flattened representation, matrix multiplication of $M_A$ with $M_B$ (with replacement) the elements of $M_B$ according to $M_A$: $M_A \cdot M_B = [0, 0, 3, 3]$.

To implement this efficient form of matrix multiplication is simple; we re-order the elements of one array by the elements of another:

```c
void Multiply(char Ma[K], char Mb[K], char Mab[K]) {
    for(int i = 0; i < K; i++) Mab[i] = Mb[Ma[i]]; }
```

Because multiplying two matrices of this form produces another matrix of this form, we always represent matrices as linear arrays indexed by state which requires only $m$ memory locations and a running time of $O(m)$.

5.5 Translating $k$-SFT to $\delta$, $\ell$ and $\phi$

To summarize, we produce the following pipeline. First, a programmer writes string manipulating functions in Bnk. Next, we compile from Bnk into an ST and then compile the ST into a $k$-SFT. Finally, we compile from the $k$-SFT to C# functions which encode $\phi$, $\delta$ and $\ell$.

These functions can then be applied as part of our data-parallel computation. As an integrated part of the pipeline, we also need a constraint solver, e.g., an SMT solver [3, 11], to construct the finite equivalence relation $\sim$ and to construct a classifier that decides membership of actual inputs in the $\sim$-equivalence classes.

Example 8 Consider again the 2-SFT in Figure 10. Recall the matrices $M_A$, $M_B$ and $M_C$ from Example 7. Let $s$ be as in Example 6. So $S = \text{map}(\text{inflate}, s) = [M_B, M_A, M_A, M_B, M_A, M_C]$ and

\[
\text{map}([\text{project, scan}(\delta, S)]) = \text{map}([I, M_B, M_B \cdot M_A, M_B \cdot M_A \cdot M_A, \ldots]) = [q_0, q_0, q_1, q_1, q_0, q_1]
\]

The rest of the output computation is the same as illustrated in Example 6.

The actual code generation to C# is discussed below. The code template for the generated C# is shown in Figure 13. The field `delta` corresponds to $\delta$, the field `lookback` corresponds to $\ell$ (lifted to symbols), and the field output corresponds to $\phi$. The semantics of `Transduce` is the implementation of `Encoder.Apply`. The implementation of `GetSymbol` uses predicates that have been generated by Z3 and then mapped to C# expressions to decide which symbol a concrete character maps to. The symbols are unique identifiers for the equivalence classes of $\sim$ as discussed above.

6. Evaluation

This section demonstrates the efficacy of our algorithms by investigating their correctness and performance. Section 6.1 explains the setup of the evaluation experiment. Section 6.2 empirically demonstrates that our generated programs produce consistent outputs compared to those available in existing system libraries. Section 6.3 provides a baseline performance comparison of our generated programs with existing library functions in the sequential case, demonstrating that our generated programs are comparable in performance. Finally, Section 6.4 demonstrates multi-factor speedups on a variety of real-world string transformation programs.

We use three encoder and decoder pairs in the following experiments. `HtmlEncode` and `HtmlDecode`, `Utf8Encode` and `Utf8Decode`, and finally, `Base64Encode` and `Base64Decode`. Each pair performs the logical inverse of the other (i.e., the output of an encoder is the input to the corresponding decoder). We also use sanitizers from the `AntiXss` library [22] in our sequential baseline comparison. All system encoders that we use are listed in Figure 11. There are several variations of some of them and they differ behaviorally. For example `HtmlEncode` in `AntiXss` is different than both the one in `HttpUtility` and the one in `WebUtility`. In particular, the latter two do not encode control characters or the replacement character `?` while the former does. However, the latter two encode all non-ASCII characters such as `ä` while the former does not encode all of them. In total, the latter two encode 101 characters out of all of the 256 extended ASCII characters, while the former encodes only 72. Since we have no bias in selecting one before the other, we compare against all of them in our experiments.

6.1 Setup

The concrete input to each individual experiment is the intermediate representation of the Bnk program under consideration. It is an ST, as an instance of the ST python class in Figure 4. For example, the Bnk intermediate representation of `Base64Encode` is shown in Figure 12. It corresponds to the ST shown in Figure 3. It has a single state $q = 0$, a register that is a pair of numbers, two transitions $\{r_1, r_2\}$ and three finalizers $\{f_1, f_2, f_3\}$. The initial register value is the pair $(0, 0)$. Notice that the function $E$ is defined as a $Z$ axiom. Such axioms are either included or used to define corresponding methods during code generation.

The python function `utf2cs` in Figure 12 is the entry point that generates the final C# code. First, it invokes `Explore` (as defined in Figure 4) to construct the equivalent (modulo grouping) SFT*. It then decomposes the transitions of the SFT* by introducing lookback and constructs a deterministic $k$-SFT. In the case of encoders whose input is assumed to be a valid UTF16 string, the resulting $k$-SFT is composed with the 2-SFT `Rsp`, as shown in Figure 8(b), to lift the input strings to arbitrary sequences of characters (as opposed to valid UTF16 strings only, recall the discussion at the end.

<table>
<thead>
<tr>
<th>Routine</th>
<th>Library</th>
</tr>
</thead>
<tbody>
<tr>
<td>HtmlEncode</td>
<td>AntiXss.AntiXssEncoder</td>
</tr>
<tr>
<td>HtmlDecode</td>
<td>AntiXss.AntiXssEncoder</td>
</tr>
<tr>
<td>CssEncode</td>
<td>AntiXss.AntiXssEncoder</td>
</tr>
<tr>
<td>JavaScriptStringEncode</td>
<td>AntiXss.AntiXssEncoder</td>
</tr>
<tr>
<td>HtmlEncode</td>
<td>System.Net.WebUtility</td>
</tr>
<tr>
<td>HtmlDecode</td>
<td>System.Net.WebUtility</td>
</tr>
<tr>
<td>ToBase64String</td>
<td>System.Convert</td>
</tr>
<tr>
<td>FromBase64String</td>
<td>System.Convert</td>
</tr>
<tr>
<td>UTF8.GetBytes (encoder)</td>
<td>System.Text.Encoding</td>
</tr>
<tr>
<td>UTF8.GetString (decoder)</td>
<td>System.Text.Encoding</td>
</tr>
</tbody>
</table>

Figure 11. Pre-existing encoders used for comparison. All encoders are from .NET Framework 4.5.
To demonstrate that our synthesized encoders are correct, we checked the consistency of the B\(_E\)K-generated output against independent implementations with the same functionality. We generated a set of 100 1-MB strings and evaluate both the independent output and the B\(_E\)K generated code on each input.

The strings are chosen randomly. We used independently-produced implementations listed in Figure 11 for comparison. In each case we implemented a corresponding equivalent B\(_E\)K program and automatically generated the code as explained above. For each individual input we compared that the output of the B\(_E\)K generated program is equal to the output returned by the corresponding system encoder. We found no discrepancies. The system encoders, listed in Figure 11, came from .NET 4.5 core libraries and the AntiXss encoder library.

### 6.3 Sequential B\(_E\)K

The generic code template for the generated sequential C\# code for a given B\(_E\)K encoder is shown in Figure 13. It exercises the same interface of the k-SFT that is used by the parallel implementation. The method Encoder.Apply implements the sequential routine. Concrete characters \(x\) are mapped to a finite set of symbols through GetSymbol. Each symbol identifies the equivalence class in which the input behaves similarly (recall the discussion from Section 5.3). The maximal lookback is \(k\). The initial state is 0. Given a state \(q\) and a symbol \(s\), \(\text{delta}[q][s]\) is the next state. Output is computed from a given state \(q\) and symbol \(s\) by invoking \(\text{output}[q][s][x_1, \ldots, x_m]\) where \((x_1, \ldots, x_m)\) is the subsequence of \(m\) previous characters, \(m = \text{lookback}[q][s]\), note that \(m \leq k\). We have not optimized for the case when the input grouping size is fixed (as with Base64Decode) but iterate one character at a time over the input. For each of the \textit{string to string} encoders in Figure 11 (the top 9 rows) we compared the running time with the corresponding B\(_E\)K generated encoder Encoder. Apply over 100 randomly generated 1-megabyte strings (over extended ASCII). To get statistically significant results, we ran each experiment 10 times and report the mean \(m\) and the standard error \(e\) of the running time as \(m(\pm e)\). For HtmlEncode we use a different version of B\(_E\)K encoder in the case of AntiXss to match the semantics, while we use another B\(_E\)K encoder for the other two libraries. For HtmlDecode we used the same B\(_E\)K encoder in all three instances. As input to the decoder we used the output from the corresponding encoder, i.e., from the random inputs we generate inputs to the decoders using the corresponding encoders: inputs for HtmlDecode in AntiXss are generated with HtmlEncode in AntiXss, inputs for HtmlDecode in WebUtility are generated with HtmlEncode in WebUtility, etc. The Html decoder in B\(_E\)K supports up to 3 digit decimal encodings, which is why we restricted this experiment to extended ASCII. We see no reason why supporting longer encodings would affect the sequential running time in any significant manner. The experiments were carried out on a Lenovo X1 Carbon laptop with Intel i7 2GHz processor having 8GB of RAM and running 64-bit Windows 8.1.

The results are shown in Figure 14. The sequential performance of our generated encoders are on par with existing hand-optimized codes. Our code is sometimes faster and sometimes slower than...
<table>
<thead>
<tr>
<th>Routine</th>
<th>Library</th>
<th>$t$(sec)</th>
<th>$t_{B_{4k}}$(sec)</th>
<th>$t_{B_{4k}}/t$</th>
</tr>
</thead>
<tbody>
<tr>
<td>HtmlEncode</td>
<td>AntiXss</td>
<td>2.7(±.02)</td>
<td>4.6(±.1)</td>
<td>1.7</td>
</tr>
<tr>
<td>HtmlDecode</td>
<td>AntiXss</td>
<td>8.0(±.1)</td>
<td>3.5(±.03)</td>
<td>0.4</td>
</tr>
<tr>
<td>CssEncode</td>
<td>AntiXss</td>
<td>3.4(±.03)</td>
<td>9.5(±.05)</td>
<td>2.8</td>
</tr>
<tr>
<td>JSSSEncode</td>
<td>AntiXss</td>
<td>3.6(±.1)</td>
<td>3.7(±.03)</td>
<td>1.0</td>
</tr>
<tr>
<td>HtmlEncode</td>
<td>WebUtility</td>
<td>6.9(±.1)</td>
<td>4.6(±.07)</td>
<td>0.7</td>
</tr>
<tr>
<td>HtmlDecode</td>
<td>WebUtility</td>
<td>11(±.2)</td>
<td>4.4(±.06)</td>
<td>0.4</td>
</tr>
<tr>
<td>HtmlEncode</td>
<td>HttpUtility</td>
<td>6.8(±.07)</td>
<td>4.5(±.04)</td>
<td>0.7</td>
</tr>
<tr>
<td>HtmlDecode</td>
<td>HttpUtility</td>
<td>11(±.1)</td>
<td>4.4(±.04)</td>
<td>0.4</td>
</tr>
<tr>
<td>JSSSEncode</td>
<td>HttpUtility</td>
<td>3.6(±.07)</td>
<td>3.8(±.05)</td>
<td>1.0</td>
</tr>
</tbody>
</table>

Geomean: 0.92

**Figure 14.** Sequential comparison over 100x1MB strings.

these standard libraries. Consider `HtmlDecode`: BEK is significantly faster than the AntiXss baseline as this decoder has many corner cases which makes it difficult to hand-optimize (and thus points to the benefits of an automated compiler). However, consider `CssEncode` where BEK is almost 3x slower AntiXss. This is because all encodings have the form `\000XY` and use the loop over function calls in output in Figure 13 to append `\` and four `0`'s to sb, one at a time. We could amortize this huge overhead through simple optimizations (i.e., inlining function calls instead of individually calling them through a table), however, because this paper is about extracting data parallelism from BEK codes with registers, we left this simple optimization for future work.

The encoder producing inputs for `HtmlDecode` in the AntiXss experiment encodes less data than in the other two `HtmlDecode` experiments, as was explained above, which explains the BEK time difference of almost 1 second in those experiments.

To summarize, the geometric mean of all speedup experiments is 0.92 and at the 95% confidence interval, ranges from 0.57 to 1.46. So our approach is neither statistically faster nor slower than these hand-optimized baselines.

### 6.4 Data Parallel BEK

In this section we demonstrate multi-factor performance improvements over sequential baselines by utilizing multiple threads on multi-core hardware. It is worth noting our approach is not limited to multiprocessors as it is data parallel and thus it can target many forms of data parallel hardware (e.g., GPUs or Hadoop clusters).

**Platform:** We conducted all experiments on an unloaded Intel 2 GHz (E5-2650) workstation with 64 GB of RAM and 32 logical processors (2 sockets with 16 physical cores).

**Inputs:** For both the HTML and UTF8 encoder/decoder pair, we encode (and then decode) a 1GB subset of Wikipedia’s HTML while for the Base64 encoder/decoder pair, we encode (and then decode) a 100 MB SQL server executable. We measured the time it takes to execute a BEK program after reading the input from disk. Many of our performance numbers are faster than a commodity disk and thus we did not want our experiments to be IO bound. To compute throughput numbers, we measure both bytes read and bytes written as both numbers are required to understand a BEK program’s performance. To get statistically significant results, we ran each experiment 10 times and reported the mean and 95% confidence interval of the mean.

**Throughput:** Our data-parallel BEK programs exploit parallel hardware and are fast. As shown in Figure 15, with 32 logical threads, our encoders and decoders are able to process data at speeds of anywhere from 250 to 600 MB/sec. In contrast, the serial baselines are anywhere from 30 to 100 MB/sec. Secondly, even with small input data (i.e., Base64 encoder only encodes 100 MB) we still see significant throughput. This implies that the cost to create and manage threads does not dominate the computation. Lastly, our single-threaded implementation is slower than the baseline. This result is pedagogical: our implementation requires each thread do two passes over the input and with a single-thread our implementation does twice as much work as the sequential baseline. A real user of our system would never run with a single thread.

**Speedup:** Our data-parallel BEK programs provide nearly linear speedups for up to 8 physical cores and moderate speedups after that, up through 16 cores. Figure 16 details the speedup of $x$ processors over a single processor. With 16 threads, our implementation is just shy of $8x$ speedup across the various encoders and decoders. Our approach saturates at 16 physical threads because the latency of reading data from shared caches and RAM becomes a bottleneck. Because our approach is data parallel, we could amortize this latency by using more physical machines such that each machine more effectively utilizes both caches and RAM. To summarize, these order-of-magnitude throughput improvements and speedups across a wide range of BEK programs are significant and enable data parallel processing of large amounts of data.

![Figure 15. Throughput of various BEK encoders shown in MB/sec on the y axis, as function of threads.](image-url)
7. Related Work

Symbolic finite transducers (SFTs) and BEK were originally introduced in [15] with a focus on security analysis of sanitizers. The formal foundations and the theoretical analysis of the underlying SFT algorithms, in particular, an algorithm for deciding equivalence of single-valued SFTs, modulo a decidable background theory is studied in [32], where Symbolic Transducers (STs) are also introduced as an extension of SFTs with registers, but exploration of STs and code generation are not studied in [15, 32]. In contrast, the focus of this paper and its motivation is efficient transformation from STs to SFTs and k-SFTs with the particular application of code generation that supports efficient parallel execution. Another recent extension of SFTs, extended SFTs [8], is SFTs with lookahead where the primary motivation is to allow lookahead without introducing registers; unlike SFTs, ESFTs are not closed under composition. The grouping idea was originally exploited in [8] where it is used as a heuristic for lifting ESFTs to SFTs, but it is not integrated with exploration. A model similar to k-SFTs is k-SLTs, k-SLTs are introduced in [7], and use lookahead instead of lookahead and, unlike ESFTs, step one symbol at a time. Our model of k-SFTs can be seen as a special class of parallelizable k-SLTs. A key property that we use here is monadicity of the predicates [33], which is needed for a k-SLTs to be translatable into a k-SFTs. The general case of deciding if a predicate is monadic is undecidable, which follows from [20, Proposition 2.b].

In recent years there has been considerable interest in automata over infinite languages [17, 30]. Finite words over an infinite alphabet are often called data words in the literature. Other related automata models are pebble automata [26] and data automata [6]. Several characterizations of logics with respect to different models of data word automata are studied in [5]. This line of work focuses on fundamental questions about definability, decidability, complexity, and expressiveness on classes of automata on one hand and fragments of logic on the other hand. A different line of work on automata with infinite alphabets introduces lattice automata [12] that are finite state automata whose transitions are labeled by elements of an atomic lattice with motivation coming from verification of symbolic communicating machines. Streaming transducers [1] is another recent symbolic extension of finite transducers. We do not know of prior work that has investigated the use of symbolic extensions of transducers for code generation.

In our implementation we use the off-the-shelf SMT solver Z3 [10] for incrementally solving label constraints that arise during the exploration algorithm. Similar applications of SMT techniques have been introduced in the context of symbolic execution of programs by using path conditions to represent under and over approximations of reachable states [13]. The distinguishing feature of our exploration algorithm is that it computes a transformation that is behaviorally equivalent to the original ST with respect to the transduction semantics, which is important for correct code generation.

Finite state transducers have been used for dynamic and static analysis to validate sanitization functions in web applications in [2]. Other types of security analyses use string analysis [24, 35]. Yu et.al. show how multiple automata can be composed to model looping code [36]. Our work is complementary to previous efforts in using SMT solvers to solve problems related to list transformations. HAMPI [18] and Kaluza [28] extend the STP solver to handle equations over strings and equations with multiple variables. We are not aware of previous work investigating the use of finite state transducers for efficient code generation. One explanation for this is that classical finite state transducers are not directly suited for this purpose because SFTs can be exponentially more succinct with respect to the alphabet size.

Parallel algorithms for finite state machines, akin to the one presented in this work, have been known for a long time [14, 19]. Like this paper, Ladner and Fischer build a parallel implementation by phrasing finite state machine computation as matrix multiplication. Their approach targets applications with small finite state machines and thus they ignore the resulting cubic (in the number of states) overhead [19]. Hillis and Steele describe an improved algorithm based on parallel prefix sum which reduces this overhead to linear in the number of states [14]. To the best of our knowledge, none of these approaches allow infinite alphabets, neither were implemented on real hardware nor are they used with a larger framework for transducing. This paper builds on these theoretical insights, fits into a larger compilation framework which lets programmers use an expressive language to write encoders and decoders, and then evaluates these programs on large scale, parallel machines.

Finally, stream processing is a programming model which organizes programs by independent filters that communicate over data channels. Programmers need not think about parallelism as it is implicit in the programming model; a streaming program is the successive composition of independent filters and the runtime maps these independent computations to hardware parallelism [31, 37].
Unlike the programming model in this paper, streaming based programming models are not analyzable nor do they break data dependencies to expose data parallelism like we do in this work. In particular, streaming languages can only run as fast as hardware can expose a stream. Thus, it is not clear how they can hide I/O from reading large files from multiple disks.

8. Conclusions
This paper demonstrates how to compile an expressive domain-specific language, BEK, to produce consistent and fast encoders and sanitizers. We use symbolic transducers as an intermediate formalism, and then introduce a novel algorithm which performs a symbolic partial exploration of these transducers to obtain simplified, stateless versions of the original BEK program.

We then show how to compile the resulting stateless transducers to data-parallel hardware. Our compilation results indicate significant runtime improvements: our data-parallel compilation speeds up by 8x faster compared to a sequential implementation, when run on a 16-node commodity desktop.

References