

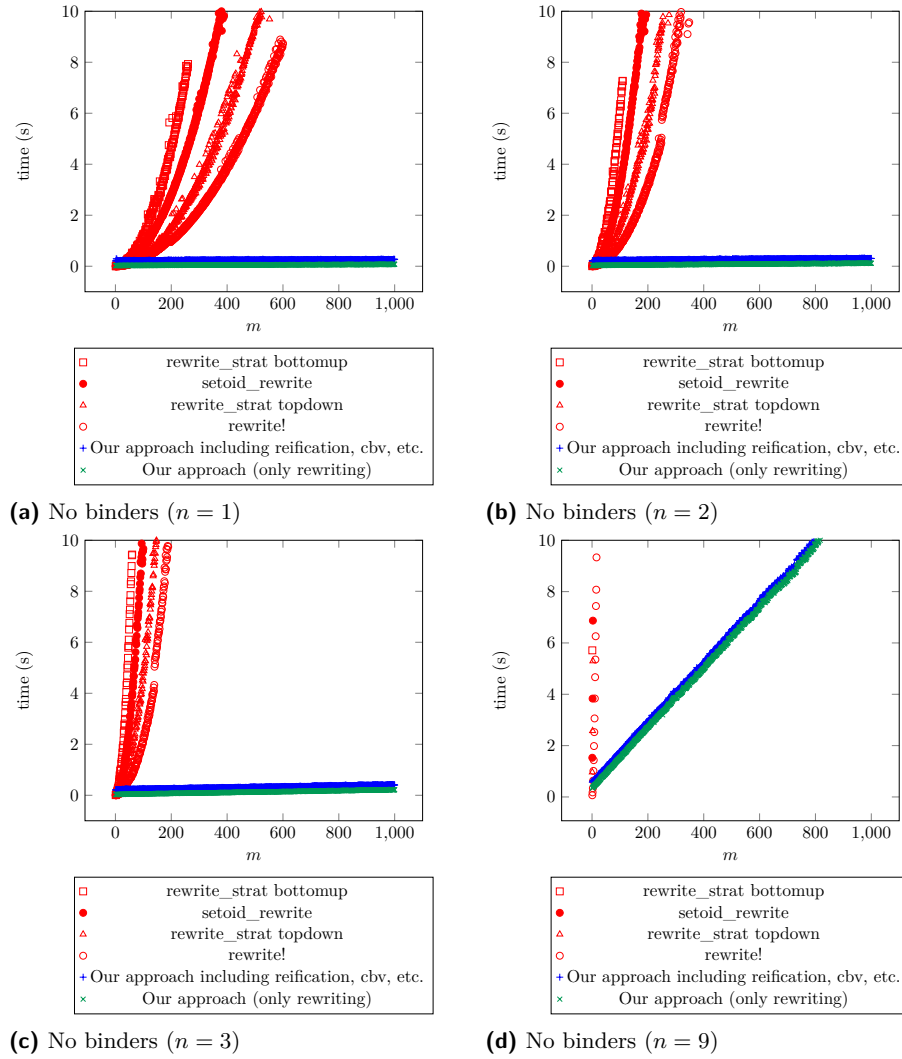
Figure 4 Timing of different partial-evaluation implementations for code with no binders for fixed m . Note that we have a logarithmic time scale, because term size is proportional to 2^n .

B Additional Benchmarking Plots

B.1 Rewriting Without Binders

The code in Figure 7a in Appendix C.1 is parameterized on both n , the height of the tree, and m , the number of rewriting occurrences per node. The plot in Figure 3a displays only the case of $n = 3$. The plots in Figure 4 display how performance scales as a factor of n for fixed m , and the plots in Figure 5 display how performance scales as a factor of m for fixed n . Note the logarithmic scaling on the time axis in the plots in Figure 4, as term size is proportional to $m \cdot 2^n$.

We can see from these graphs and the ones in Figure 5 that (a) we incur constant overhead over most of the other methods, which dominates on small examples; (b) when the term is quite large and there are few opportunities for rewriting relative to the term size (i.e., $m \leq 2$), we are worse than `rewrite !Z.add_0_r` but still better than the other methods;



■ **Figure 5** Timing of different partial-evaluation implementations for code with no binders for fixed n (1, 2, 3, and then we jump to 9)

23:24 Accelerating Verified-Compiler Development with a Verified Rewriting Engine

776 and (c) when there are many opportunities for rewriting relative to the term size ($m > 2$),
777 we thoroughly dominate the other methods.

778 B.2 Additional Information on the Fiat Cryptography Benchmark

779 The data for this benchmark can be found on GitHub at `mit-plv/fiat-crypto@perf-`
780 `testing-data-ITP-2022-rewriting`.

781 It may also be useful to see performance results with absolute times, rather than normalized
782 execution ratios vs. the original Fiat Cryptography implementation. Furthermore, the
783 benchmarks fit into four quite different groupings: elements of the cross product of two
784 algorithms (unsaturated Solinas and word-by-word Montgomery) and bitwidths of target
785 architectures (32-bit or 64-bit). Here we provide absolute-time graphs by grouping in Figure 6.

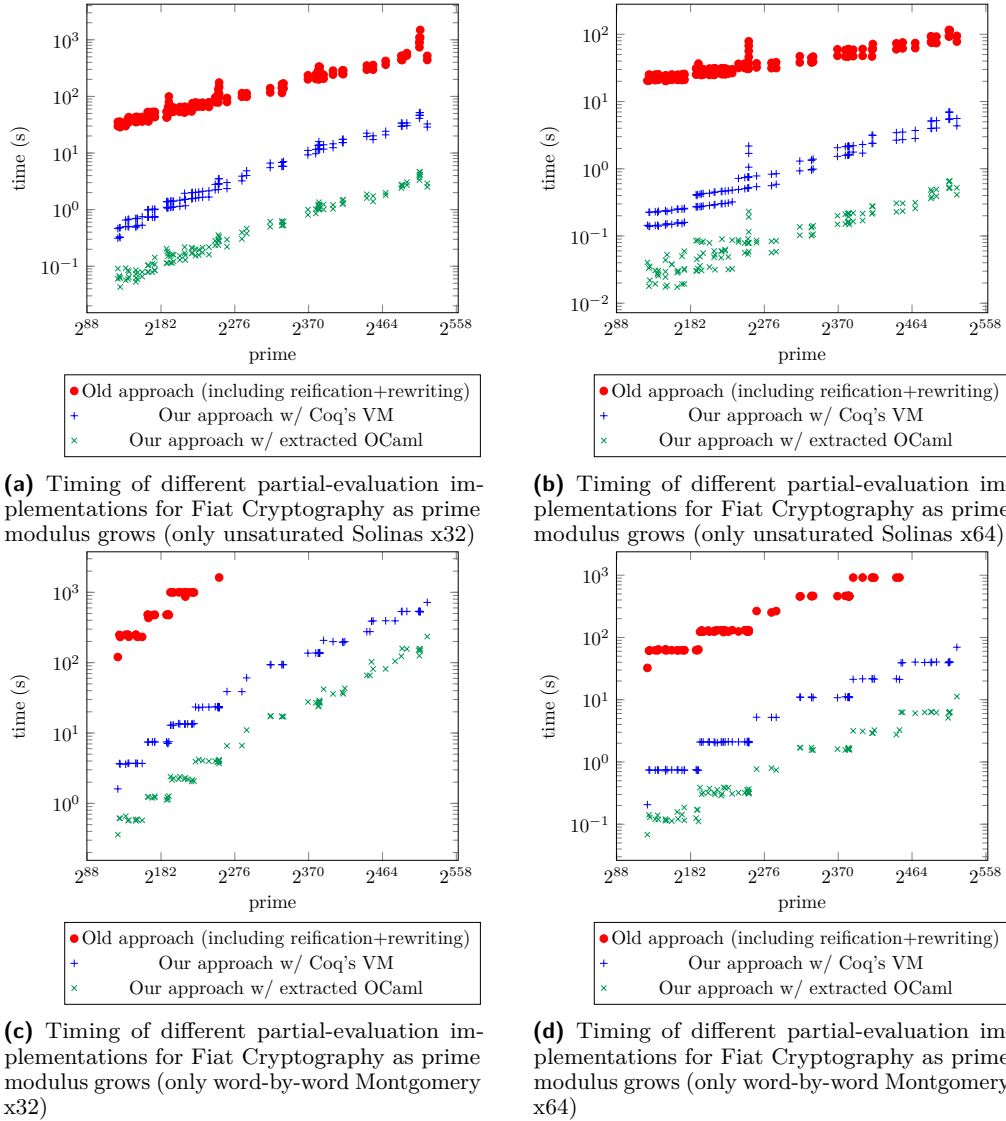


Figure 6 Timing of different partial-evaluation implementations for Fiat Cryptography vs. prime modulus

$\text{iter}_m(v) = v + \underbrace{0 + 0 + \dots + 0}_m$	<code>let v₁ := v₀ + v₀ + 0 in</code>
$\text{tree}_{0,m}(v) = \text{iter}_m(v + v)$	<code>:</code>
$\text{tree}_{n+1,m}(v) = \text{iter}_m(\text{tree}_{n,m}(v) + \text{tree}_{n,m}(v))$	<code>let v_n := v_{n-1} + v_{n-1} + 0 in</code>
	<code>v_n + v_n + 0</code>
(a) Expressions computing initial code for Rewriting Without Binders	(b) Initial code for Rewriting Under Binders

■ **Figure 7** Code for rewriting without and under binders

786 C Additional Information on Microbenchmarks

787 We performed all benchmarks on a 3.5 GHz Intel Haswell running Linux and Coq 8.11.1.
 788 We name the subsections here with the names that show up in the code supplement.

789 C.1 Rewriting Without Binders: Plus0Tree

790 Consider the code defined by the expression $\text{tree}_{n,m}(v)$ in Figure 7a. We want to remove all
 791 of the $+0$ s. There are $\Theta(m \cdot 2^n)$ such rewriting locations. We can start from this expression
 792 directly, in which case reification alone takes as much time as Coq's `rewrite`. As the
 793 reification method was not especially optimized, and there exist fast reification methods [10],
 794 we instead start from a call to a recursive function that generates such an expression.

795 We use two definitions for this microbenchmark:

```

Definition iter (m : nat) (acc v : Z) :=
  @nat_rect (fun _ => Z -> Z)
    (fun acc => acc)
    (fun _ rec acc => rec (acc + v))
    m
    acc.

Definition make_tree (n m : nat) (v acc : Z) :=
  Eval cbv [iter] in
  @nat_rect (fun _ => Z * Z -> Z)
    (fun '(v, acc) => iter m (acc + acc) v)
    (fun _ rec '(v, acc) =>
      iter m (rec (v, acc) + rec (v, acc)) v)
    n
    (v, acc).
```

796 C.2 Rewriting Under Binders: UnderLetsPlus0

797 Consider now the code in Figure 7b, which is a version of the code above where redundant
 798 expressions are shared via `let` bindings.

799 The code used to define this microbenchmark is

```

Definition make_lets_def (n:nat) (v acc : Z) :=
  @nat_rect (fun _ => Z * Z -> Z)
    (fun '(v, acc) => acc + acc + v)
    (fun _ rec '(v, acc) =>
      dlet acc := acc + acc + v in rec (v, acc))
    n
    (v, acc).
```

We note some details of the rewriting framework that were glossed over in the main body of the paper, which are useful for using the code: Although the rewriting framework does not support dependently typed constants, we can automatically preprocess uses of eliminators like `nat_rect` and `list_rect` into nondependent versions. The tactic that does this preprocessing is extensible via \mathcal{L}_{tac} 's reassignment feature. Since pattern-matching compilation mixed with NbE requires knowing how many arguments a constant can be applied to, we must internally use a version of the recursion principle whose type arguments do not contain arrows; current preprocessing can handle recursion principles with either no arrows or one arrow in the motive. Even though we will eventually plug in 0 for v , we jump through some extra hoops to ensure that our rewriter cannot cheat by rewriting away the $+ 0$ before reducing the recursion on n .

We can reduce this expression in three ways.

C.2.1 Our Rewriter

One lemma is required for rewriting with our rewriter:

```
Lemma Z.add_0_r : forall z, z + 0 = z.
```

Creating the rewriter takes about 12 seconds on the machine we used for running the performance experiments:

```
Make myrew := Rewriter For (Z.add_0_r, eval_rect nat, eval_rect prod).
```

Recall from Section 2 that `eval_rect` is a definition provided by our framework for eagerly evaluating recursion associated with certain types. It functions by triggering typeclass resolution for the lemmas reducing the recursion principle associated to the given type. We provide instances for `nat`, `prod`, `list`, `option`, and `bool`. Users may add more instances if they desire.

C.2.2 setoid_rewrite and rewrite_strat

To give as many advantages as we can to the preexisting work on rewriting, we pre-reduce the recursion on `nats` using `cbv` before performing `setoid_rewrite`. (Note that `setoid_rewrite` cannot itself perform reduction without generating large proof terms, and `rewrite_strat` is not currently capable of sequencing reduction with rewriting internally due to bugs such as #10923.) Rewriting itself is easy; we may use any of `repeat setoid_rewrite Z.add_0_r`, `rewrite_strat topdown Z.add_0_r`, or `rewrite_strat bottomup Z.add_0_r`.

C.3 Binders and Recursive Functions: LiftLetsMap

The next experiment uses the code in Figure 8. Note that the `let ... in ...` binding blocks further reduction of `map_dbl` when we iterate it m times in `make`, and so we need to take care to preserve sharing when reducing here.

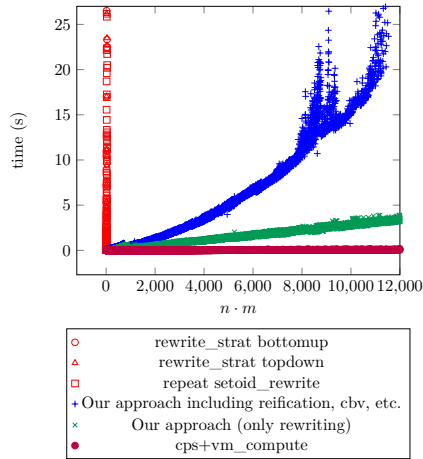
Figure 9 compares performance between our approach, `repeat setoid_rewrite`, and two variants of `rewrite_strat`. Additionally, we consider another option, which was adopted by Fiat Cryptography at a larger scale: rewrite our functions to improve reduction behavior. Specifically, both functions are rewritten in continuation-passing style, which makes them harder to read and reason about but allows standard VM-based reduction to achieve good performance. The figure shows that `rewrite_strat` variants are essentially unusable for this example, with `setoid_rewrite` performing only marginally better, while our approach

$$\text{map_dbl}(\ell) = \begin{cases} [] & \text{if } \ell = [] \\ \text{let } y := h + h \text{ in } y :: \text{map_dbl}(t) & \text{if } \ell = h :: t \end{cases}$$

$$\text{make}(n, m, v) = \begin{cases} [v, \dots, v]_n & \text{if } m = 0 \\ \text{map_dbl}(\text{make}(n, m - 1, v)) & \text{if } m > 0 \end{cases}$$

$$\text{example}_{n,m} = \forall v, \text{make}(n, m, v) = []$$

■ **Figure 8** Initial code for binders and recursive functions



■ **Figure 9** Benchmark with recursive functions

applied to the original, more readable definitions loses ground steadily to VM-based reduction on CPS'd code. On the largest terms ($n \cdot m > 20,000$), the gap is 6s vs. 0.1s of compilation time, which should often be acceptable in return for simplified coding and proofs, plus the ability to mix proved rewrite rules with built-in reductions. Note that about 99% of the difference between the full time of our method and just the rewriting is spent in the final **cbv** at the end, used to denote our output term from reified syntax. We blame this performance on the unfortunate fact that reduction in Coq is quadratic in the number of nested binders present; see Coq bug #11151. This bug has since been fixed, as of Coq 8.14; see Coq PR #13537.

We can perform this rewriting in four ways.

C.3.1 Our Rewriter

One lemma is required for rewriting with our rewriter:

```
Lemma eval_repeat A x n
: @List.repeat A x ('n) = ident.eagerly nat_rect _ [] (λ k repeat_k, x :: repeat_k) ('n).
```

Recall that the apostrophe marker (') is explained in Subsection 4.3. Recall again from Section 2 that we use **ident.eagerly** to ask the reducer to simplify a case of primitive recursion by complete traversal of the designated argument's constructor tree. Our current version only allows a limited, hard-coded set of eliminators with **ident.eagerly** (**nat_rect** on return types with either zero or one arrows, **list_rect** on return types with either zero or one arrows, and **List.nth_default**), but nothing in principle prevents automatic generation of the necessary code.

We construct our rewriter with

```
Make myrew := Rewriter For (eval_repeat, eval_rect list, eval_rect nat)
(with extra_idents (Z.add)).
```

On the machine we used for running all our performance experiments, this command takes about 13 seconds to run. Note that all identifiers which appear in any goal to be rewritten must either appear in the type of one of the rewrite rules or in the tuple passed to **with extra_idents**.

Rewriting is relatively simple, now. Simply invoke the tactic **Rewrite_for myrew**. We support rewriting on only the left-hand-side and on only the right-hand-side using either the tactic **Rewrite_lhs_for myrew** or else the tactic **Rewrite_rhs_for myrew**, respectively.

C.3.2 rewrite_strat

To reduce adequately using **rewrite_strat**, we need the following two lemmas:

```
Lemma lift_let_list_rect T A P N C (v : A) fls
: @list_rect T P N C (Let_In v fls) = Let_In v (fun v => @list_rect T P N C (fls v)).
Lemma lift_let_cons T A x (v : A) f
: @cons T x (Let_In v f) = Let_In v (fun v => @cons T x (f v)).
```

Note that **Let_In** is the constant we use for writing **let ... in ...** expressions that do not reduce under ζ . Throughout most of this paper, anywhere that **let ... in ...** appears, we have actually used **Let_In** in the code. It would alternatively be possible to extend the reification preprocessor to automatically convert **let ... in ...** to **Let_In**, but this may cause problems when converting the interpretation of the reified term with the prereified term, as Coq's conversion does not allow fine-tuning of when to inline or unfold **lets**.

874 To rewrite, we start with `cbv [example make map_dbl]` to expose the underlying term
 875 to rewriting. One would hope that one could just add these two hints to a database `db`
 876 and then write `rewrite_strat (repeat (eval cbn [list_rect]; try bottomup hints`
 877 `db))`, but unfortunately this does not work due to a number of bugs in Coq: #10934, #10923,
 878 #4175, #10955, and the potential to hit #10972. Instead, we must put the two lemmas in sepa-
 879 rate databases, and then write `repeat (cbn [list_rect]; (rewrite_strat (try repeat`
 880 `bottomup hints db1)); (rewrite_strat (try repeat bottomup hints db2)))`. Note
 881 that the rewriting with `lift_let_cons` can be done either top-down or bottom-up, but
 882 `rewrite_strat` breaks if the rewriting with `lift_let_list_rect` is done top-down.

883 C.3.3 CPS and the VM

884 If we want to use Coq's built-in VM reduction without our rewriter, to achieve the prior
 885 state-of-the-art performance, we can do so on this example, because it only involves partial
 886 reduction and not equational rewriting. However, we must (a) module-opacify the constants
 887 which are not to be unfolded, and (b) rewrite all of our code in CPS.

888 Then we are looking at

$$\begin{aligned}
 \text{map_dbl_cps}(\ell, k) &= \begin{cases} k([]) & \text{if } \ell = [] \\ \text{let } y := h +_{\text{ax}} h \text{ in } & \text{if } \ell = h :: t \\ \text{map_dbl_cps}(t, & \\ (\lambda ys, k(y :: ys))) & \end{cases} \\
 \text{make_cps}(n, m, v, k) &= \begin{cases} k(\underbrace{[v, \dots, v]}_n) & \text{if } m = 0 \\ \text{make_cps}(n, m - 1, v, & \text{if } m > 0 \\ (\lambda \ell, \text{map_dbl_cps}(\ell, k)) & \end{cases} \\
 \text{example_cps}_{n,m} &= \forall v, \text{ make_cps}(n, m, v, \lambda x. x) = []
 \end{aligned}$$

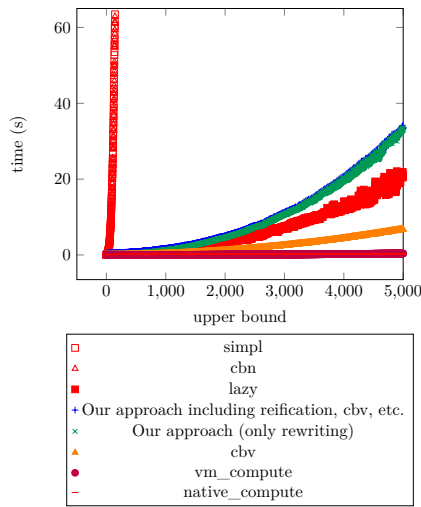
891
 892 Then we can just run `vm_compute`. Note that this strategy, while quite fast, results in
 893 a stack overflow when $n \cdot m$ is larger than approximately $2.5 \cdot 10^4$. This is unsurprising,
 894 as we are generating quite large terms. Our framework can handle terms of this size but
 895 stack-overflows on only slightly larger terms.
 896

897 C.3.4 Takeaway

898 From this example, we conclude that `rewrite_strat` is unsuitable for computations involving
 899 large terms with many binders, especially in cases where reduction and rewriting need to
 900 be interwoven, and that the many bugs in `rewrite_strat` result in confusing gymnastics
 901 required for success. The prior state of the art—writing code in CPS—suitably tweaked
 902 by using module opacity to allow `vm_compute`, remains the best performer here, though
 903 the cost of rewriting everything in CPS may be prohibitive. Our method soundly beats
 904 `rewrite_strat`. We are additionally bottlenecked on `cbv`, which is used to unfold the goal
 905 post-rewriting and costs about a minute on the largest of terms; see Coq bug #11151 for a
 906 discussion on what is wrong with Coq's reduction here.

907 C.4 SieveOfEratosthenes

908 The final experiment involves full reduction in computing the Sieve of Eratosthenes, taking
 909 inspiration on benchmark choice from Aehlig et al. [1]. We find in Figure 10 that we are



■ **Figure 10** Full evaluation, Sieve of Eratosthenes

910 slower than `vm_compute`, `native_compute`, and `cbv`, but faster than `lazy`, and of course
 911 much faster than `simpl` and `cbn`, which are quite slow.

912 We define the sieve using `PositiveMap.t` and `list Z`:

```

Definition sieve' (fuel : nat) (max : Z) :=
  List.rev
    (fst
      (@nat_rect
        (λ _, list Z (* primes *) *
          PositiveSet.t (* composites *) *
          positive (* np (next_prime) *) ->
          list Z (* primes *) *
          PositiveSet.t (* composites *)
        ) (λ '(primes, composites, next_prime),
          (primes, composites))
        ) (λ _ rec '(primes, composites, np),
          rec
            (if (PositiveSet.mem np composites ||
              (Z.pos np >? max))%bool%Z
            then
              (primes, composites, Pos.succ np)
            else
              (Z.pos np :: primes,
                List.fold_right
                  PositiveSet.add
                    composites
                    (List.map
                      (λ n, Pos.mul (Pos.of_nat (S n)) np)
                      (List.seq 0 (Z.to_nat(max/Z.pos np)))),
                  Pos.succ np)))
          fuel
          (nil, PositiveSet.empty, 2%positive))).

Definition sieve (n : Z)
  := Eval cbv [sieve'] in sieve' (Z.to_nat n).
```

913 We need four lemmas and an additional instance to create the rewriter:

```
Lemma eval_fold_right A B f x ls :
@List.fold_right A B f x ls
= ident.eagerly list_rect _ _
  x
  (λ l ls fold_right_ls, f l fold_right_ls)
  ls.
```

```
Lemma eval_app A xs ys :
xs ++ ys
= ident.eagerly list_rect A _
  ys
  (λ x xs app_xs_ys, x :: app_xs_ys)
  xs.
```

```
Lemma eval_map A B f ls :
@List.map A B f ls
= ident.eagerly list_rect _ _
  []
  (λ l ls map_ls, f l :: map_ls)
  ls.
```

```
Lemma eval_rev A xs :
@List.rev A xs
= (@list_rect _ (fun _ => _))
  []
  (λ x xs rev_xs, rev_xs ++ [x])%list
  xs.
```

Scheme Equality for PositiveSet.tree.

```
Definition PositiveSet_t_beq
: PositiveSet.t -> PositiveSet.t -> bool
:= tree_beq.
```

```
Global Instance PositiveSet_reflect_eqb
: reflect_rel (@eq PositiveSet.t) PositiveSet_t_beq
:= reflect_of_brel
  internal_tree_dec_bl internal_tree_dec_lb.
```

914 We then create the rewriter with

```
Make myrew := Rewriter For
  (eval_rect nat, eval_rect prod, eval_fold_right,
   eval_map, do_again eval_rev, eval_rect bool,
   @fst_pair, eval_rect list, eval_app)
  (with extra identfs (Z.eqb, orb, Z.gtb,
   PositiveSet.elements, @fst, @snd,
   PositiveSet.mem, Pos.succ, PositiveSet.add,
   List.fold_right, List.map, List.seq, Pos.mul,
   S, Pos.of_nat, Z.to_nat, Z.div, Z.pos, 0,
   PositiveSet.empty))
  (with delta).
```

915 To get **cbn** and **simpl** to unfold our term fully, we emit

```
Global Arguments Pos.to_nat !_ / .
```

916 **D** Fusing Compiler Passes

917 When we moved the constant-folding rules from `??` from before abstract interpretation to
 918 after it, the performance of our compiler on Word-by-Word Montgomery code synthesis
 919 decreased significantly. (The generated code did not change.) We discovered that the number
 920 of variable assignments in our intermediate code was quartic in the number of bits in the
 921 prime, while the number of variable assignments in the generated code is only quadratic.
 922 The performance numbers we measured supported this theory: the overall running time
 923 of synthesizing code for a prime near 2^k jumped from $\Theta(k^2)$ to $\Theta(k^4)$ when we made this
 924 change. We believe that fusing abstract interpretation with rewriting and partial evaluation
 925 would allow us to fix this asymptotic-complexity issue.

926 To make this situation more concrete, consider the following example: Fiat Cryptography
 927 uses abstract interpretation to perform bounds analysis; each expression is associated with
 928 a range that describes the lower and upper bounds of values that expression might take
 929 on. Abstract interpretation on addition works as follows: if we have that $x_\ell \leq x \leq x_u$ and
 930 $y_\ell \leq y \leq y_u$, then we have that $x_\ell + y_\ell \leq x + y \leq x_u + y_u$. Performing bounds analysis
 931 on $+$ requires two additions. We might have an arithmetic simplification that says that
 932 $x + y = x$ whenever we know that $0 \leq y \leq 0$. If we perform the abstract interpretation and
 933 then the arithmetic simplification, we perform two additions (for the bounds analysis) and
 934 then two comparisons (to test the lower and upper bounds of y for equality with 0). We
 935 cannot perform the arithmetic simplification before abstract interpretation, because we will
 936 not know the bounds of y . However, if we perform the arithmetic simplification for each
 937 expression after performing bounds analysis on its *subexpressions* and only after this perform
 938 abstract interpretation on the resulting expression, then we need not use any additions to
 939 compute the bounds of $x + y$ when $0 \leq y \leq 0$, since the expression will just become x .

940 Another essential pass to fuse with rewriting and partial evaluation is let-lifting. Unless
 941 all of the code is CPS-converted ahead of time, attempting to do let-lifting via rewriting,
 942 as must be done when using `setoid_rewrite`, `rewrite_strat`, or \mathcal{R}_{tac} , results in slower
 943 asymptotics. This pattern is already apparent in the `LiftLetsMap` / “Binders and Recursive
 944 Functions” example in Appendix C.3. We achieve linear performance in $n \cdot m$ when ignoring
 945 the final `cbv`, while `setoid_rewrite` and `rewrite_strat` are both cubic. The rewriter in
 946 \mathcal{R}_{tac} cannot possibly achieve better than $\mathcal{O}(n \cdot m^2)$ unless it can be sublinear in the number
 947 of rewrites, because our rewriter gets away with a constant number of rewrites (four), plus
 948 evaluating recursion principles for a total amount of work $\mathcal{O}(n \cdot m)$. But without primitive
 949 support for let-lifting, it is instead necessary to lift the lets by rewrite rules, which requires
 950 $\mathcal{O}(n \cdot m^2)$ rewrites just to lift the lets. The analysis is thus: running `make` simply gives us
 951 m nested applications of `map_dbl` to a length- n list. To reduce a given call to `map_dbl`, all
 952 existing let-binders must first be lifted (there are $n \cdot k$ of them on the k -innermost-call) across
 953 `map_dbl`, one-at-a-time. Then the `map_dbl` adds another n let binders, so we end up doing
 954 $\sum_{k=0}^m n \cdot k$ lifts, i.e., $n \cdot m(m+1)/2$ rewrites just to lift the lets.

955 **E** Experience vs. Lean and `setoid_rewrite`

956 Although all of our toy examples work with `setoid_rewrite` or `rewrite_strat` (until the
 957 terms get too big), even the smallest of examples in Fiat Cryptography fell over using these
 958 tactics. When attempting to use `setoid_rewrite` for partial evaluation and rewriting on
 959 unsaturated Solinas with 1 limb on small primes (such as $2^{61} - 1$), we were able to get
 960 `setoid_rewrite` to finish after about 100 seconds. Trying to synthesize code for two limbs

on slightly larger primes (such as $2^{107} - 1$, which needs two limbs on a 64-bit machine) took about 10 minutes; three limbs took just under 3.5 hours, and four limbs failed to synthesize with an out-of-memory error after using over 60 GB of RAM. The widely used primes tend to have around five to ten limbs. See #13576 for more details and for updates.

The `rewrite_strat` tactic, which does not require duplicating the entire goal at each rewriting step, fared a bit better. Small primes with 1 limb took about 90 seconds, but further performance tuning of the typeclass instances dropped this time down to 11 seconds. The bugs in `rewrite_strat` made finding the right magic invocation quite painful, nonetheless; the invocation we settled on involved *sixteen* consecutive calls to `rewrite_strat` with varying arguments and strategies. Two limbs took about 90 seconds, three limbs took a bit under 10 minutes, and four limbs took about 70 minutes and about 17 GB of RAM. Extrapolating out the exponential asymptotics of the fastest-growing subcall to `rewrite_strat` indicates that 5 limbs would take 11–12 hours, 6 limbs would take 10–11 days, 7 limbs would take 31–32 weeks, 8 limbs would take 13–14 years, 9 limbs would take 2–3 centuries, 10 limbs would take 6–7 millennia, and 15 limbs would take 2–3 times the age of the universe, and 17 limbs, the largest example we might find at present in the real world, would take over $1000\times$ the age of the universe! See #13708 for more details and updates.

This experiment using `rewrite_strat` can be found online in the Coq source file at `src/fiat_crypto_via_setoid_rewrite_standalone.v` on GitHub at `coq-community/coq-performance-tests`. To test with the two-limb prime $2^{107} - 1$, change `Goal goal` to `Goal goal_of_size 2%nat` near the bottom of the file.

We also tried Lean, in the hopes that rewriting in Lean, specifically optimized for performance, would be up to the challenge. Although Lean performed about 30% better than Coq’s `setoid_rewrite` on the 1-limb example, taking a bit under a minute, it did not complete on the two-limb example even after four hours (after which we stopped trying), and a five-limb example was still going after 40 hours.

Our experiments with running `rewrite` in Lean on the Fiat Cryptography code can be found in the file `fiat-crypto-lean/src/fiat_crypto.lean` on GitHub at `mit-plv/fiat-crypto@lean`. We used Lean version 3.4.2, commit `cbd2b6686ddb`, Release. Run `make` in `fiat-crypto-lean` to run the one-limb example; change `open ex` to `open ex2` to try the two-limb example, or to `open ex5` to try the five-limb example.

F Limitations and Preprocessing

We now note some details of the rewriting framework that were previously glossed over, which are useful for using the code or implementing something similar, but which do not add fundamental capabilities to the approach. Although the rewriting framework does not support dependently typed constants, we can automatically preprocess uses of eliminators like `nat_rect` and `list_rect` into nondependent versions. The tactic that does this preprocessing is extensible via \mathcal{L}_{tac} ’s reassignment feature. Since pattern-matching compilation mixed with NbE requires knowing how many arguments a constant can be applied to, internally we must use a version of the recursion principle whose type arguments do not contain arrows; current preprocessing can handle recursion principles with either no arrows or one arrow in motives.

Recall from Section 2 that `eval_rect` is a definition provided by our framework for eagerly evaluating recursion associated with certain types. It functions by triggering typeclass resolution for the lemmas reducing the recursion principle associated to the given type. We provide instances for `nat`, `prod`, `list`, `option`, and `bool`. Users may add more instances if they desire.

Recall again from Section 2 that we use `ident.eagerly` to ask the reducer to simplify a case of primitive recursion by complete traversal of the designated argument's constructor tree. Our current version only allows a limited, hard-coded set of eliminators with `ident.eagerly` (`nat_rect` on return types with either zero or one arrows, `list_rect` on return types with either zero or one arrows, and `List.nth_default`), but nothing in principle prevents automatic generation of the necessary code.

We define a constant `Let_In` which we use for writing `let ... in ...` expressions that do not reduce under ζ (Coq's reduction rule for `let`-inlining). Throughout most of this paper, anywhere that `let ... in ...` appears, we have actually used `Let_In` in the code. It would alternatively be possible to extend the reification preprocessor to automatically convert `let ... in ...` to `Let_In`, but this strategy may cause problems when converting the interpretation of the reified term with the prereified term, as Coq's conversion does not allow fine-tuning of when to inline or unfold `lets`.

G Reading the Code Supplement

We have attached both the code for implementing the rewriter, as well as a copy of Fiat Cryptography adapted to use the rewriting framework. Both code supplements build with Coq versions 8.9–8.13, and they require that whichever OCaml was used to build Coq be installed on the system to permit building plugins. (If Coq was installed via `opam`, then the correct version of OCaml will automatically be available.) Both code bases can be built by running `make` in the top-level directory.

The performance data for both repositories are included at the top level as `.txt` and `.csv` files.

The performance data for the microbenchmarks can be rebuilt using `make perf-SuperFast perf-Fast perf-Medium` followed by `make perf-csv` to get the `.txt` and `.csv` files. The microbenchmarks should run in about 24 hours when run with `-j5` on a 3.5 GHz machine. There also exist targets `perf-Slow` and `perf-VerySlow`, but these take significantly longer.

The performance data for the macrobenchmark can be rebuilt from the Fiat Cryptography copy included by running `make perf -k`. We ran this with `PERF_MAX_TIME=3600` to allow each benchmark to run for up to an hour; the default is 10 minutes per benchmark. Expect the benchmarks to take over a week of time with an hour timeout and five cores. Some tests are expected to fail, making `-k` a necessary flag. Again, the `perf-csv` target will aggregate the logs and turn them into `.txt` and `.csv` files.

The entry point for the rewriter is the Coq source file `rewriter/src/Rewriter/Util/plugins/RewriterBuild.v`.

The rewrite rules used in Fiat Cryptography are defined in `fiat-crypto/src/Rewriter/Rules.v` and proven in `fiat-crypto/src/Rewriter/RulesProofs.v`. Note that the Fiat Cryptography copy uses `COQPATH` for dependency management, and `.dir-locals.el` to set `COQPATH` in `emacs/PG`; you must accept the setting when opening a file in the directory for interactive compilation to work. Thus interactive editing either requires `ProofGeneral` or manual setting of `COQPATH`. The correct value of `COQPATH` can be found by running `make printenv`.

We will now go through this paper and describe where to find each reference in the code base.

G.1 Code from Section 1, Introduction

The P-384 curve is mentioned. This is the curve with modulus $2^{384} - 2^{128} - 2^{96} + 2^{32} - 1$; its benchmarks can be found in files matching the glob `fiat-crypto/src/Rewriter/PerfTesting/Specific/generated/p2384m2128m296p232m1__*__word_by_word_montgomery_*`. The output `.log` files are included in the tarball; the `.v` and `.sh` files are automatically generated in the course of running `make perf -k`.

G.1.1 Code from Subsection 1.1, Related Work

There is no code mentioned in this section.

G.1.2 Code from Subsection 1.2, Our Solution

We claimed that our solution meets five criteria. We briefly justify each criterion with a sentence or a pointer to code:

- We claimed that we **did not grow the trusted code base**. In any example file (of which a couple can be found in `rewriter/src/Rewriter/Rewriter/Examples/`), the `Make` command creates a rewriter package. Running `Print Assumptions` on this new constant (often named `rewriter` or `myrew`) should demonstrate a lack of axioms. `Print Assumptions` may also be run on the proof that results from using the rewriter.
- We claimed **fast** partial evaluation with reasonable memory use; we assume that the performance graphs stand on their own to support this claim. Note that memory usage can be observed by making the benchmarks while passing `TIMED=1` to `make`.
- We claimed to allow reduction that *mixes rules of the definitional equality with equalities proven explicitly as theorems*; the “rules of the definitional equality” are, for example, β reduction, and we assert that it should be self-evident that our rewriter supports this.
- We claimed to allow **rapid iteration** on rewrite rules with *minimal verification overhead*. We invite the reader to alter the list of constants in any of the `Make ... := Rewriter For ...` invocations in `rewriter/src/Rewriter/Rewriter/Examples/` or to alter the list of rewrite rules in `fiat-crypto/src/Rewriter/Rules.v` to experience iteration on rewrite rules.
- We claimed common-subterm **sharing preservation**. This is implemented by supporting the use of the `dlet` notation which is defined in `rewriter/src/Rewriter/Util/LetIn.v` via the `Let_In` constant. We will come back to the infrastructure that supports this.
- We claimed **extraction of standalone partial evaluators**. The extraction is performed in the files `perf_unsaturated_solinas.v` and `perf_word_by_word_montgomery.v`, and the files `saturated_solinas.v`, `unsaturated_solinas.v`, and `word_by_word_montgomery.v`, all in the directory `fiat-crypto/src/ExtractionOCaml/`. The OCaml code can be extracted and built using the target `make standalone-ocaml` (or `make perf-standalone` for the `perf_` binaries). There may be some issues with building these binaries on Windows as some versions of `ocaml-opt` on Windows seem not to support outputting binaries without the `.exe` extension.

We mention encoding pattern matching explicitly by adopting the performance-tuned approach of Maranget [17]; the code for this is in `rewriter/src/Rewriter/Rewriter/Rewriter.v` starting from the comment above `Inductive decision_tree` and including the Gallina definitions `eval_decision_tree` and `compile_rewrites`.

We mention integration with abstract interpretation; the abstract-interpretation pass is implemented in `fiat-crypto/src/AbstractInterpretation/`; integration is achieved in

1094 rewrite rules in `fiat-crypto/src/Rewriter/Rules.v` making use of the various `Local Notations`
 1095 defined in that file for `ident.cast`.

1096 We mention parametric higher-order abstract syntax (PHOAS); the definition of our
 1097 datatype is `Inductive expr` in module `Compilers.expr` in `rewriter/src/Rewriter/Language/`
 1098 `Language.v`. We mention a let-lifting transformation threaded throughout reduction; this
 1099 is `Inductive UnderLets`, a monad defined in module `Compilers.UnderLets` in the file
 1100 `rewriter/src/Rewriter/Language/UnderLets.v`.

1101 G.2 Code from Section 2, A Motivating Example

1102 The `prefixSums` example appears in the Coq source file `rewriter/src/Rewriter/Rewriter/`
 1103 `Examples/PrefixSums.v`. Note that we use `dlet` rather than `let` in binding `acc'` so that
 1104 we can preserve the `let` binder even under ι reduction, which much of Coq's infrastructure
 1105 performs eagerly. Because we do not depend on the axiom of functional extensionality, we
 1106 also in practice require `Proper` instances for each higher-order identifier saying that each
 1107 constant respects function extensionality. Although we glossed over this detail in the body
 1108 of this paper, we also prove

```
Global Instance: forall A B,
  Proper ((eq ==> eq ==> eq) ==> eq ==> eq ==> eq)
    (@fold_left A B).
```

1109 The `Make` command is exposed in `rewriter/src/Rewriter/Util/plugins/RewriterBuild.v`
 1110 and defined in `rewriter/src/Rewriter/Util/plugins/rewriter_build_plugin.mlg`. Note
 1111 that one must run `make` to create this latter file; it is copied over from a version-specific file
 1112 at the beginning of the build.

1113 The `do_again`, `eval_rect`, and `ident.eagerly` constants are defined at the bottom of
 1114 module `RewriteRuleNotations` in `rewriter/src/Rewriter/Language/Pre.v`.

1115 G.3 Code from Section 3, The Structure of a Rewriter

1116 G.3.1 Code from Subsection 3.1, Our Approach in Ten Steps

1117 We match the nine steps with functions from the source code:

- 1118 1. The given lemma statements are scraped for which named functions and types the
 1119 rewriter package will support. This is performed by `rewriter_scrape_data` in the file
 1120 `rewriter/src/Rewriter/Util/plugins/rewriter_build.ml` which invokes the \mathcal{L}_{tac}
 1121 tactic named `make_scrape_data` in a submodule in the source file `rewriter/src/`
 1122 `Rewriter/Language/IdentifiersBasicGenerate.v` on a goal headed by the constant we
 1123 provide under the name `Pre.ScrapedData.t_with_args` in `rewriter/src/Rewriter/`
 1124 `Language/PreCommon.v`.
- 1125 2. Inductive types enumerating all available primitive types and functions are emitted.
 1126 This step is performed by `rewriter_emit_inductives` in file `rewriter/src/Rewriter/`
 1127 `Util/plugins/rewriter_build.ml` invoking tactics, like `make_base_elim` in `rewriter/`
 1128 `src/Rewriter/Language/IdentifiersBasicGenerate.v`, on goals headed by constants
 1129 from `rewriter/src/Rewriter/Language/IdentifiersBasicLibrary.v`, including the
 1130 constant `base_elim_with_args` for example, to turn scraped data into eliminators for the
 1131 inductives. The actual emitting of inductives is performed by code in the file `rewriter/`
 1132 `src/Rewriter/Util/plugins/inductive_from_elim.ml`.
- 1133 3. Tactics generate all of the necessary definitions and prove all of the necessary lemmas for
 1134 dealing with this particular set of inductive codes. This step is performed by the tactic

1135 `make_rewriter_of_scraped_and_ind` in the source file `rewriter/src/Rewriter/Util/`
 1136 `plugins/rewriter_build.ml` which invokes the tactic `make_rewriter_all` defined in
 1137 the file `rewriter/src/Rewriter/Rewriter/AllTactics.v` on a goal headed by the pro-
 1138 vided constant `VerifiedRewriter_with_ind_args` defined in `rewriter/src/Rewriter/`
 1139 `Rewriter/ProofsCommon.v`. The definitions emitted can be found by looking at the tactic
 1140 `Build_Rewriter` in `rewriter/src/Rewriter/Rewriter/AllTactics.v`, the \mathcal{L}_{tac} tactics
 1141 `build_package` in `rewriter/src/Rewriter/Language/IdentifiersBasicGenerate.v`
 1142 and also in `rewriter/src/Rewriter/Language/IdentifiersGenerate.v` (there is a dif-
 1143 ferent tactic named `build_package` in each of these files), and `prove_package_proofs_via`
 1144 which can be found in `rewriter/src/Rewriter/Language/IdentifiersGenerateProofs.v`.

- 1145 4. The statements of rewrite rules are reified and soundness and syntactic-well-formedness
 1146 lemmas are proven about each of them. This is done as part of the previous step, when
 1147 the tactic `make_rewriter_all` transitively calls `Build_Rewriter` from `rewriter/src/`
 1148 `Rewriter/Rewriter/AllTactics.v`. Reification is handled by the tactic `Build_RewriterT`
 1149 in `rewriter/src/Rewriter/Rewriter/Reify.v`, while soundness and the syntactic-well-
 1150 formedness proofs are handled by the tactics `prove_interp_good` and `prove_good` respec-
 1151 tively, both in the source file `rewriter/src/Rewriter/Rewriter/ProofsCommonTactics.v`.
- 1152 5. The definitions needed to perform reification and rewriting and the lemmas needed to
 1153 prove correctness are assembled into a single package that can be passed by name to the
 1154 rewriting tactic. This step is also performed by `make_rewriter_of_scraped_and_ind`
 1155 in the source file `rewriter/src/Rewriter/Util/plugins/rewriter_build.ml`.

1156 When we want to rewrite with a rewriter package in a goal, the following steps are
 1157 performed, with code in the following places:

- 1158 1. We rearrange the goal into a closed logical formula: all free-variable quantification in
 1159 the proof context is replaced by changing the equality goal into an equality between
 1160 two functions (taking the free variables as inputs). Note that it is not actually an
 1161 equality between two functions but rather an `equiv` between two functions, where `equiv`
 1162 is a custom relation we define indexed over type codes that is equality up to function
 1163 extensionality. This step is performed by the tactic `generalize_hyps_for_rewriting`
 1164 in `rewriter/src/Rewriter/Rewriter/AllTactics.v`.
- 1165 2. We reify the side of the goal we want to simplify, using the inductive codes in the
 1166 specified package. That side of the goal is then replaced with a call to a denotation
 1167 function on the reified version. This step is performed by the tactic `do_reify_rhs_with`
 1168 in `rewriter/src/Rewriter/Rewriter/AllTactics.v`.
- 1169 3. We use a theorem stating that rewriting preserves denotations of well-formed terms to
 1170 replace the denotation subterm with the denotation of the rewriter applied to the same
 1171 reified term. We use Coq's built-in full reduction (`vm_compute`) to reduce the application
 1172 of the rewriter to the reified term. This step is performed by the tactic `do_rewrite_with`
 1173 in `rewriter/src/Rewriter/Rewriter/AllTactics.v`.
- 1174 4. Finally, we run `cbv` (a standard call-by-value reducer) to simplify away the invocation of
 1175 the denotation function on the concrete syntax tree from rewriting. This step is performed
 1176 by the tactic `do_final_cbv` in `rewriter/src/Rewriter/Rewriter/AllTactics.v`.

1177 These steps are put together in the tactic `Rewrite_for_gen` in `rewriter/src/Rewriter/`
 1178 `Rewriter/AllTactics.v`.

1179 The expression language e corresponds to the inductive `expr` type defined in the module
 1180 `Compilers.expr` in `rewriter/src/Rewriter/Language/Language.v`.

1181 Our Approach in More Than Nine Steps

1182 As the nine steps of Subsection 3.1 do not exactly match the code, we describe here a more
 1183 accurate version of what is going on. For ease of readability, we do not clutter this description
 1184 with references to the code supplement, instead allowing the reader to match up the steps
 1185 here with the more coarse-grained ones in Subsection 3.1 or Appendix G.3.1.

1186 In order to allow easy invocation of our rewriter, a great deal of code (about 6500 lines)
 1187 needed to be written. Some of this code is about reifying rewrite rules into a form that the
 1188 rewriter can deal with them in. Other code is about proving that the reified rewrite rules
 1189 preserve interpretation and are well-formed. We wrote some plugin code to automatically
 1190 generate the inductive type of base-type codes and identifier codes, as well as the two variants
 1191 of the identifier-code inductive used internally in the rewriter. One interesting bit of code
 1192 that resulted was a plugin that can emit an inductive declaration given the Church encoding
 1193 (or eliminator) of the inductive type to be defined. We wrote a great deal of tactic code to
 1194 prove basic properties about these inductive types, from the fact that one can unify two
 1195 identifier codes and extract constraints on their type variables from this unification, to the
 1196 fact that type codes have decidable equality. Additional plugin code was written to invoke
 1197 the tactics that construct these definitions and prove these properties, so that we could
 1198 generate an entire rewriter from a single command, rather than having the user separately
 1199 invoke multiple commands in sequence.

1200 In order to build the precomputed rewriter, the following actions are performed:

- 1201 1. The terms and types to be supported by the rewriter package are scraped from the given
 1202 lemmas.
- 1203 2. An inductive type of codes for the types is emitted, and then three different versions of
 1204 inductive codes for the identifiers are emitted (one with type arguments, one with type
 1205 arguments supporting pattern type variables, and one without any type arguments, to be
 1206 used internally in pattern-matching compilation).
- 1207 3. Tactics generate all of the necessary definitions and prove all of the necessary lemmas
 1208 for dealing with this particular set of inductive codes. Definitions cover categories like
 1209 “Boolean equality on type codes” and “how to extract the pattern type variables from a
 1210 given identifier code,” and lemma categories include “type codes have decidable equality”
 1211 and “the types being coded for have decidable equality” and “the identifiers all respect
 1212 function extensionality.”
- 1213 4. The rewrite rules are reified, and we prove interpretation-correctness and well-formedness
 1214 lemmas about each of them.
- 1215 5. The definitions needed to perform reification and rewriting and the lemmas needed to
 1216 prove correctness are assembled into a single package that can be passed by name to the
 1217 rewriting tactic.
- 1218 6. The denotation functions for type and identifier codes are marked for early expansion in
 1219 the kernel via the **Strategy** command; this is necessary for conversion at **Qed**-time to
 1220 perform reasonably on enormous goals.

1221 When we want to rewrite with a rewriter package in a goal, the following steps are
 1222 performed:

- 1223 1. We use **etransitivity** to allow rewriting separately on the left- and right-hand-sides
 1224 of an equality. Note that we do not currently support rewriting in non-equality goals,
 1225 but this is easily worked around using `let v := open_constr:(_) in replace <some
 1226 term> with v` and then rewriting in the second goal.

2. We revert all hypotheses mentioned in the goal, and change the form of the goal from a universally quantified statement about equality into a statement that two functions are extensionally equal. Note that this step will fail if any hypotheses are functions not known to respect function extensionality via typeclass search.
3. We reify the side of the goal that is not an existential variable using the inductive codes in the specified package; the resulting goal equates the denotation of the newly reified term with the original `evvar`.
4. We use a lemma stating that rewriting preserves denotations of well-formed terms to replace the goal with the rewriter applied to our reified term. We use `vm_compute` to prove the well-formedness side condition reflectively. We use `vm_compute` again to reduce the application of the rewriter to the reified term.
5. Finally, we run `cbv` to unfold the denotation function, and we instantiate the `evvar` with the resulting rewritten term.

There are a couple of steps that contribute to the trusted code base. We must trust that the rewriter package we generate from the rewrite rules in fact matches the rewrite rules we want to rewrite with. This involves partially trusting the scraper, the reifier, and the glue code. We must also trust the VM we use for reduction at various points in rewriting. Otherwise, everything is checked by Coq.

G.3.2 Code from Subsection 3.2, Pattern-Matching Compilation and Evaluation

The pattern-matching compilation step is done by the tactic `CompileRewrites` in `rewriter/src/Rewriter/Rewriter/Rewriter.v`, which just invokes the Gallina definition named `compile_rewrites` with ever-increasing amounts of fuel until it succeeds. (It should never fail for reasons other than insufficient fuel, unless there is a bug in the code.) The workhorse function here is `compile_rewrites_step`.

The decision-tree evaluation step is done by the definition `eval_rewrite_rules`, also in the file `rewriter/src/Rewriter/Rewriter/Rewriter.v`. The correctness lemmas are the theorem `eval_rewrite_rules_correct` in the file `rewriter/src/Rewriter/Rewriter/InterpProofs.v` and the theorem `wf_eval_rewrite_rules` in `rewriter/src/Rewriter/Rewriter/Wf.v`. Note that the second of these lemmas, not mentioned in the paper, is effectively saying that for two related syntax trees, `eval_rewrite_rules` picks the same rewrite rule for both. (We actually prove a slightly weaker lemma, which is a bit harder to state in English.)

The third step of rewriting with a given rule is performed by the definition `rewrite_with_rule` in `rewriter/src/Rewriter/Rewriter/Rewriter.v`. The correctness proof goes by the name `interp_rewrite_with_rule` in `rewriter/src/Rewriter/Rewriter/InterpProofs.v`. Note that the well-formedness-preservation proof for this definition is inlined into the proof of the lemma `wf_eval_rewrite_rules` mentioned above.

The inductive description of decision trees is `decision_tree` in `rewriter/src/Rewriter/Rewriter/Rewriter.v`.

The pattern language is defined as the inductive `pattern` in `rewriter/src/Rewriter/Rewriter/Rewriter.v`. Note that we have a `Raw` version and a typed version; the pattern-matching compilation and decision-tree evaluation of Aehlig et al. [1] is an algorithm on untyped patterns and untyped terms. We found that trying to maintain typing constraints led to headaches with dependent types. Therefore when doing the actual decision-tree evaluation, we wrap all of our expressions in the dynamically typed `rawexpr` type and all of our patterns

1273 in the dynamically typed `Raw.pattern` type. We also emit separate inductives of identifier
 1274 codes for each of the `expr`, `pattern`, and `Raw.pattern` type families.

1275 We partially evaluate the partial evaluator defined by `eval_rewrite_rules` in the \mathcal{L}_{tac}
 1276 tactic `make_rewrite_head` in `rewriter/src/Rewriter/Rewriter/Reify.v`.

1277 G.3.3 Code from Subsection 3.3, Adding Higher-Order Features

1278 The type NbE_t mentioned in this paper is not actually used in the code; the version we
 1279 have is described in Subsection 4.2 as the definition `value'` in `rewriter/src/Rewriter/
 1280 Rewriter/Rewriter.v`.

1281 The functions `reify` and `reflect` are defined in `rewriter/src/Rewriter/Rewriter/
 1282 Rewriter.v` and share names with the functions in the paper. The function `reduce` is named
 1283 `rewrite_bottomup` in the code, and the closest match to NbE is `rewrite`.

1284 G.4 Code from Section 4, Scaling Challenges

1285 G.4.1 Code from Subsection 4.1, Variable Environments Will Be Large

1286 The inductives `type`, `base_type` (actually the inductive type `base.type.type` in the sup-
 1287 plemental code), and `expr`, as well as the definition `Expr`, are all defined in `rewriter/src/
 1288 Rewriter/Language/Language.v`. The definition `denoteT` is the fixpoint type `interp` (the
 1289 fixpoint `interp` in the module `type`) in `rewriter/src/Rewriter/Language/Language.v`.
 1290 The definition `denoteE` is `expr.interp`, and `DenoteE` is the fixpoint `expr.interp`.

1291 As mentioned above, `nbeT` does not actually exist as stated but is close to `value'` in
 1292 `rewriter/src/Rewriter/Rewriter/Rewriter.v`. The functions `reify` and `reflect` are
 1293 defined in `rewriter/src/Rewriter/Rewriter/Rewriter.v` and share names with the func-
 1294 tions in the paper. The actual code is somewhat more complicated than the version presented
 1295 in the paper, due to needing to deal with converting well-typed-by-construction expres-
 1296 sions to dynamically typed expressions for use in decision-tree evaluation and also due
 1297 to the need to support early partial evaluation against a concrete decision tree. Thus
 1298 the version of `reflect` that actually invokes rewriting at base types is a separate defini-
 1299 tion `assemble_identifier_rewriters`, while `reify` invokes a version of `reflect` (named
 1300 `reflect`) that does not call rewriting. The function named `reduce` is what we call
 1301 `rewrite_bottomup` in the code; the name `Rewrite` is shared between this paper and the code.
 1302 Note that we eventually instantiate the argument `rewrite_head` of `rewrite_bottomup` with a
 1303 partially evaluated version of the definition named `assemble_identifier_rewriters`. Note
 1304 also that we use `fuel` to support `do_again`, and this is used in the definition `repeat_rewrite`
 1305 that calls `rewrite_bottomup`.

1306 The correctness proofs are `InterpRewrite` in the Coq source file `rewriter/src/Rewriter/
 1307 Rewriter/InterpProofs.v` and `Wf_Rewrite` in `rewriter/src/Rewriter/Rewriter/Wf.v`.

1308 Packages containing rewriters and their correctness theorems are in the record `VerifiedRewriter`
 1309 in `rewriter/src/Rewriter/Rewriter/ProofsCommon.v`; a package of this type is then
 1310 passed to the tactic `Rewrite_for_gen` from `rewriter/src/Rewriter/Rewriter/AllTactics.v`
 1311 to perform the actual rewriting. The correspondence of the code to the various steps in
 1312 rewriting is described in the second list of Appendix G.3.1.

1313 G.4.2 Code from Subsection 4.2, Subterm Sharing Is Crucial

1314 To run the P-256 example in the copy of Fiat Cryptography attached as a code supplement,
 1315 after building the library, run the code

```
Require Import Crypto.Rewriter.PerfTesting.Core.
Require Import Crypto.Util.Option.
```

```
Import WordByWordMontgomery.
Import Core.RuntimeDefinitions.
```

```
Definition p : params
:= Eval compute in invert_Some (of_string "2^256-2^224+2^192+2^96-1" 64).
```

```
Goal True.
```

```
  (* Successful run: *)
```

```
  Time let v := (eval cbv
    -[Let_In
      runtime_nth_default
      runtime_add runtime_sub runtime_mul runtime_opp runtime_div runtime_modulo
      RT_Z.add_get_carry_full RT_Z.add_with_get_carry_full RT_Z.mul_split]
    in (GallinaDefOf p)) in
    idtac.
```

```
  (* Unsuccessful OOM run: *)
```

```
  Time let v := (eval cbv
    -[(*Let_In*)
      runtime_nth_default
      runtime_add runtime_sub runtime_mul runtime_opp runtime_div runtime_modulo
      RT_Z.add_get_carry_full RT_Z.add_with_get_carry_full RT_Z.mul_split]
    in (GallinaDefOf p)) in
    idtac.
```

```
Abort.
```

1316 The UnderLets monad is defined in the file `rewriter/src/Rewriter/Language/UnderLets.v`.

1317 The definitions `nbeT'`, `nbeT`, and `nbeT_with_lets` are in `rewriter/src/Rewriter/`

1318 `Rewriter/Rewriter.v` and are named `value'`, `value`, and `value_with_lets`, respectively.

1319 G.4.3 Code from Subsection 4.3, Rules Need Side Conditions

1320 The “variant of pattern variable that only matches constants” is actually special support
 1321 for the reification of `ident.literal` (defined in the module `RewriterRuleNotations` in
 1322 `rewriter/src/Rewriter/Language/Pre.v`) threaded throughout the rewriter. The apos-
 1323 trophe notation `'` is also introduced in the module `RewriterRuleNotations` in `rewriter/`
 1324 `src/Rewriter/Language/Pre.v`. The support for side conditions is handled by permit-
 1325 ting rewrite-rule-replacement expressions to return `option expr` instead of `expr`, allow-
 1326 ing the function `expr_to_pattern_and_replacement` in the file `rewriter/src/Rewriter/`
 1327 `Rewriter/Reify.v` to fold the side conditions into a choice of whether to return `Some` or
 1328 `None`.

1329 G.4.4 Code from Subsection 4.4, Side Conditions Need Abstract 1330 Interpretation

1331 The abstract-interpretation pass is defined in `fiat-crypto/src/AbstractInterpretation/`
 1332 `,` and the rewrite rules handling abstract-interpretation results are the Gallina definitions
 1333 `arith_with_casts_rewrite_rulesT`, as well as `strip_literal_casts_rewrite_rulesT`,
 1334 as well as `fancy_with_casts_rewrite_rulesT`, and finally as well as `mul_split_rewrite_rulesT`,
 1335 all defined in `fiat-crypto/src/Rewriter/Rules.v`.

1336 The `clip` function is the definition `ident.cast` in `fiat-crypto/src/Language/PreExtra.v`.

1337 G.5 Code from Section 5, Evaluation

1338 G.5.1 Code from Subsection 5.1, Iteration on the Fiat Cryptography 1339 Compiler

1340 The old continuation-passing-style versions of verified arithmetic functions can be found in
1341 the folder `fiat-crypto/src/ArithmeticCPS/`, while the new versions can be found in the
1342 folder `fiat-crypto/src/Arithmetic/`.

1343 The rewrite rules from `??`, `??` can be found in the definition `arith_rewrite_rulesT`
1344 starting at the comment “We reassociate some multiplication of small constants” in `fiat-`
1345 `crypto/src/Rewriter/Rules.v`.

1346 The frontend constructs from `??`, `??` are in `all_ident_named_interped` defined in `fiat-`
1347 `crypto/src/Language/IdentifierParameters.v`.

1348 ■ The multiplication primitives are `with_name ident_Z_mul_split Z.mul_split` as well
1349 as `with_name ident_Z_mul_high Z.mul_high`, as well as the various Coq expressions
1350 `with_name ident_fancy_mulXX ident.fancy.mulXX` for each `X` being either `l` or `h`.

1351 ■ The “comment” function is both `with_name ident_comment (@ident.comment)` as well
1352 as `with_name ident_comment_no_keep (@ident.comment_no_keep)`.

1353 ■ The bitwise exclusive-or is `with_name ident_Z_lxor Z.lxor`.

1354 ■ The special identity function which prints in the backend as a call to some inline assembly
1355 is `with_name ident_value_barrier (@Z.value_barrier)`.

1356 The rules about bitmasking operations from `??`, `??` can be found in `arith_with_casts_rewrite_rulesT`
1357 in `fiat-crypto/src/Rewriter/Rules.v` and involve `Z.land` and `Z.lor`.

1358 The compiler configuration about conditional-move instructions is the flag `-cmovznz-`
1359 `by-mul` defined in `fiat-crypto/src/CLI.v`. The if-statement using the thus-defined
1360 `use_mul_for_cmovznz` is in `src/PushButtonSynthesis/Primitives.v`.

1361 The rewrite rules for the new backends mentioned in `??`, `??` are defined by `fancy_with_casts_rewrite_rulesT`
1362 and `mul_split_rewrite_rulesT` as well as `multiret_split_rewrite_rulesT` and `noselect_rewrite_rulesT`
1363 in `fiat-crypto/src/Rewriter/Rules.v`. The special function `Z.combine_at_bitwidth` is
1364 defined in `fiat-crypto/src/Util/ZUtil/Definitions.v`. The designation of `Z.combine_at_bitwidth`
1365 as an identifier that should be inlined occurs by listing it in the definition `var_like_ids`
1366 in `fiat-crypto/src/Language/IdentifierParameters.v`.

1367 The rules involving carries mentioned in `??`, `??` and Appendix D, Fusing Compiler Passes
1368 are in `arith_with_casts_rewrite_rulesT` in `fiat-crypto/src/Rewriter/Rules.v`.

1369 G.5.2 Code from Subsection 5.2, Microbenchmarks

1370 This code is found in the files in `rewriter/src/Rewriter/Rewriter/Examples/`. We
1371 ran the microbenchmarks using the code in `rewriter/src/Rewriter/Rewriter/Examples/`
1372 `PerfTesting/Harness.v` together with some Makefile cleverness.

1373 The code for Figure 3a from Appendix C.1, Rewriting Without Binders: `Plus0Tree` can
1374 be found in `Plus0Tree.v`.

1375 The code for Figure 3b from Appendix C.2, Rewriting Under Binders: `UnderLetsPlus0`
1376 can be found in `UnderLetsPlus0.v`.

1377 The code for Figure 9 from Appendix C.3, Binders and Recursive Functions: `LiftLetsMap`
1378 can be found in `LiftLetsMap.v`.

1379 The code for Figure 10 from Appendix C.4, SieveOfEratosthenes can be found in
1380 `SieveOfEratosthenes.v`.

1381 G.5.3 Code from Subsection 5.3, Macrobenchmark: Fiat Cryptography

1382 The rewrite rules are defined in `fiat-crypto/src/Rewriter/Rules.v` and proven in the file
 1383 `fiat-crypto/src/Rewriter/RulesProofs.v`. They are turned into rewriters in the various
 1384 files in `fiat-crypto/src/Rewriter/Passes/`. The shared inductives and definitions are
 1385 defined in the Coq source file `fiat-crypto/src/Language/IdentifiersBasicGENERATED.v`,
 1386 the Coq source file `fiat-crypto/src/Language/IdentifiersGENERATED.v`, and finally also
 1387 the Coq source file `fiat-crypto/src/Language/IdentifiersGENERATEDProofs.v`. Note
 1388 that we invoke the subtactics of the `Make` command manually to increase parallelism in the
 1389 build and to allow a shared language across multiple rewriter packages.

1390 G.6 Code from Appendix F, Limitations and Preprocessing

1391 The \mathcal{L}_{tac} hooks for extending the preprocessing of eliminators are `reify_preprocess_extra`
 1392 and `reify_ident_preprocess_extra` in a submodule of `rewriter/src/Rewriter/Language/`
 1393 `PreCommon.v`. These hooks are called by `reify_preprocess` and `reify_ident_preprocess`
 1394 in a submodule of `rewriter/src/Rewriter/Language/Language.v`. Some recursion lem-
 1395 mas for use with these tactics are defined in the `Thunked` module in `fiat-crypto/src/`
 1396 `Language/PreExtra.v`. These tactics are overridden in the file `fiat-crypto/src/Language/`
 1397 `IdentifierParameters.v`.

1398 The typeclass associated to `eval_rect` (c.f. Appendix G.2) is `rules_proofs_for_eager_type`
 1399 defined in `rewriter/src/Rewriter/Language/Pre.v`. The instances we provide by default
 1400 are defined in a submodule of `src/Rewriter/Language/PreLemmas.v`.

1401 The hard-coding of the eliminators for use with `ident.eagerly` (c.f. Appendix G.2)
 1402 is done in the tactics `reify_ident_preprocess` and `rewrite_interp_eager` in `rewriter/`
 1403 `src/Rewriter/Language/Language.v`, in the inductive type `restricted_ident` and the
 1404 typeclass `BuildEagerIdentT` in `rewriter/src/Rewriter/Language/Language.v`, and in
 1405 the \mathcal{L}_{tac} tactic with the name of `handle_reified_rewrite_rules_interp` defined in the
 1406 file `rewriter/src/Rewriter/Rewriter/ProofsCommonTactics.v`.

1407 The `Let_In` constant is defined in `rewriter/src/Rewriter/Util/LetIn.v`.