```
theory Diff_Arr_Safe_PDF
  imports Diff_Arr
begin

context
begin

qualified definition lookup where
  "lookup arr i = do {
    len ← Diff_Arr.length arr;
    if i < len
    then Diff_Arr.lookup arr i
    else return (undefined(i - len))
  }"

qualified definition update where
  "update arr i v = do {
    len ← Diff_Arr.length arr;
    if i < len
    then Diff_Arr.update arr i v
    else return arr
  }"

lemma lookup_safe [sep_heap_rules]:
  "<master_assn t * ↑(t ⊢ xs ∼ a)>
     lookup a i
  <λr. master_assn t * ↑(r = xs!i)>"

lemma update_safe [sep_heap_rules]:
  "<master_assn t * ↑(t ⊢ xs ∼ diff_arr)>
     update diff_arr i v
  <λdiff_arr. ∃A t'. master_assn t' *
    ↑((∀xs' diff_arr'. t ⊢ xs' ∼ diff_arr' ⟶ t' ⊢ xs' ∼ diff_arr')
      ∧ (t' ⊢ xs[i := v] ∼ diff_arr))>"

end

end
```