Galois Connection (20 pts)

Consider the monotonic abstraction function $\alpha : C \to A$ and concretization function $\gamma : A \to C$ forming a Galois connection between the complete lattices C and A. Let $\bigsqcup, \bigsqcap$ respectively be the least upper bound and the greatest lower bound operators in A. $\bigcup, \bigcap$ are similarly defined for C. $\subseteq$, and $\sqsubseteq$ are the ordering relations between the elements in C and A respectively.

1. Prove that for every $L_C \subseteq C$, $\alpha(\bigcup L_C) = \bigsqcup_{c \in L_C} \alpha(c)$ holds. **[5 pts]**

Let LUB_A correspond to the Least Upper Bound of A,
GLB_A correspond to the Greatest Lower Bound of A,
LUB_C correspond to the Least Upper Bound of C,
and GLB_C correspond to the Greatest Lower Bound of C.

Let $\subseteq_C$ correspond to the ordering relation between elements in C.
Let $\subseteq_A$ correspond to the ordering relation between elements in A.

We want to prove that for every set L_C which is a subset of C, applying the abstraction function α to $LUB_C(L_C)$ is equal to taking the LUB_A of applying the abstraction function α to all values in L_C.

Let $x = LUB_C(L_C)$. That is, for all $c \in L_C$, $c \subseteq_C x$. In addition, $x \subseteq_C X$, for all X that are upper bounds of L_C.

Let $y = LUB_A(\alpha(\forall c \in L_C))$. That is, for all α(c), $\alpha(c) \subseteq_A y$. In addition, $y \subseteq_A Y$, for all Y that are upper bounds of $\alpha(\forall c \in L_C)$.

Since α and γ form a Galois connection, $\forall x \in C$, $\forall z \in A$, $\alpha(x) \subseteq_A z \Leftrightarrow x \subseteq_C \gamma(z)$.

That is, each $c \in L_C$, corresponds to a specific element in C, and that ordering is preserved when each c is abstracted to $\alpha(c) \in A$.

Thus, $\alpha(LUB_C(L_C)) = LUB_A(\alpha(\forall c \in L_C))$, which is what we wanted to show.

2. Prove that for every $L_A \subseteq A$, $\gamma(\bigsqcap L_A) = \bigcap_{a \in L_A} \gamma(a)$ holds. **[5 pts]**

Let LUB_A correspond to the Least Upper Bound of A,
GLB_A correspond to the Greatest Lower Bound of A,
LUB_C correspond to the Least Upper Bound of C,
and GLB_C correspond to the Greatest Lower Bound of C.

Let $\subseteq_C$ correspond to the ordering relation between elements in C.
Let $\subseteq_A$ correspond to the ordering relation between elements in A.

We want to prove that for every set L_A which is a subset of A, applying the concretization function γ to $GLB_A(L_A)$ is equal to taking the GLB_C of applying the concretization function γ to all values in L_A.

Let $x = GLB_A(L_A)$. That is, for all $a \in L_A$, $a \subseteq_A x$. In addition, $x \subseteq_A X$, for all X that are upper bounds of L_C.

Let $y = GLB_C(\gamma(\forall a \in L_a))$. That is, for all γ(a), $\gamma(a) \subseteq_A y$. In addition, $y \subseteq_C Y$, for all Y that are upper bounds of $\gamma(\forall a \in L_A)$.

Since α and γ form a Galois connection, $\forall x \in C$, $\forall z \in A$, $\alpha(x) \subseteq_A z \Leftrightarrow x \subseteq_C \gamma(z)$.

That is, each $a \in L_A$, corresponds to a specific element in A, and that ordering is preserved when each a is abstracted to $\gamma(a) \in C$.

Thus, $\gamma(GLB_A(L_A)) = GLB_C(\gamma(\forall a \in L_a))$, which is what we wanted to show.

3. Prove that $\gamma(a) = \bigcup\{c \in C \mid \alpha(c) \sqsubseteq a\}$ holds for all $a \in A$. **[5 pts]**

Since α and γ form a Galois connection, $\forall x \in C$, $\forall z \in A$, $\alpha(x) \subseteq_A z \Leftrightarrow x \subseteq_C \gamma(z)$.

Fix $a \in A$ to an arbitrary value. Let $B = \{ c \in C \mid \alpha(c) \subseteq_A a \}$, and $b = LUB_C(B)$.

b is the least upper bound of the set of all $c \in C$, where $\alpha(c) \subseteq_A a$. We also know that $c \subseteq_C \gamma(a)$.

By the definition of a least upper bound, If $S \subseteq P$ then

- $x \in P$ is an upper bound of S if $\forall y \in S$, $y \leq x$
- $x \in P$ is the least upper bound of S if
    - x is an upper bound of S, and
    - $x \leq y$ for all upper bounds y of S

If $\gamma(a) \subset_C b$, then there exists an $e \in B$ where $a \subset_A \alpha(e)$. However, if $e \in B$, then $\alpha(e) \subseteq_A a$, which is a contradiction.
If $b \subset_C \gamma(a)$, then there exists an $f \in C$ where $\alpha(f) \subseteq_A a$, but f is not in B. This is a contradiction.

Thus, it must be true that $\gamma(a) = b = LUB_C(\{ c \in C \mid \alpha(c) \subseteq_A a \})$, which is what we wanted to show.

4. Let $F_0, F_1 : C \to C$ be two monotone functions, and let $F_0^{\#}, F_1^{\#} : A \to A$ be two functions that over-approximate them, that is such that $F_0 \circ \gamma \subseteq \gamma \circ F_o^{\#}$ and $F_1 \circ \gamma \subseteq \gamma \circ F_1^{\#}$. Then prove that $F_0 \circ F_1$, can be over-approximated by $F_0^{\#} \circ F_1^{\#}$. **[5 pts]**

γ : A -> C is a concretization function.

This means $F_0^{\#}$ over-approximates F_0, and $F_1^{\#}$ over-approximates F_1.

That means for any a ∈ A, $F_0(\gamma(a)) \subseteq \gamma(F_0^{\#}(a))$, and $F_1(\gamma(a)) \subseteq \gamma(F_1^{\#}(a))$

Fix a ∈ A as an arbitrary value. Let b = $F_0(F_1(\gamma(a)))$

Since $F_1(\gamma(a)) \subseteq \gamma(F_1^{\#}(a))$, we know that $F_0(F_1(\gamma(a))) \subseteq F_0(\gamma(F_1^{\#}(a)))$

Since $F_0(\gamma(a)) \subseteq \gamma(F_0^{\#}(a))$, we know that $F_0(F_1(\gamma(a))) \subseteq F_0(\gamma(F_1^{\#}(a))) \subseteq \gamma(F_0^{\#}(F_1^{\#}(a)))$

Thus, $F_0(F_1(\gamma(a))) \subseteq \gamma(F_0^{\#}(F_1^{\#}(a)))$

This means $F_0 \circ F_1$ can be over-approximated by $F_0^{\#} \circ F_1^{\#}$, which is what we wanted to show.

Interval Transformers (20 pts)

5. Let $f : \mathbb{R} \cup \{-\infty, +\infty\} \to \mathbb{R} \cup \{-\infty, +\infty\}$ be a monotonically increasing function with $f(-\infty) = -\infty$ and $f(\infty) = \infty$. Write sound and most precise interval abstract transformer $f^\sharp : A_I \to A_I$ for f where A_I denotes the set of all intervals over extended real numbers ($\mathbb{R} \cup \{-\infty, +\infty\}$). Also formally prove the soundness of $f^\sharp$ and show it is indeed the most precise interval transformer.
Hint: To prove soundness, first define the setwise concrete function $f_C : 2^{\mathbb{R}} \to 2^{\mathbb{R}}$ as $f_C(\mathscr{X}) = \{f(x) \mid x \in \mathscr{X}\}$, and then show that $\forall a \in A_I, f_C(\gamma(a)) \subseteq \gamma(f^\sharp(a))$. **[10 pts]**

A transformer $F^\#$ is sound if and only if $\forall z \in A$, $F(\gamma(z)) \subseteq_C \gamma(F^\#(z))$

A transformer $F^\#_{Best}$ is sound and best if for all other sound transformers, $F^\#$, $F^\#$ is not more precise than $F^\#_{Best}$. That is, $\forall z \in A$, $\gamma(F^\#_{Best}(z)) \subseteq_C \gamma(F^\#(z))$

Let $[x, y] \in A_I$, where x and y are the interval's lower bounds and upper bounds, respectively. Define $F^\#([x, y]) = [F(x), F(y)]$

Let $F_C : 2^{\mathbb{R}} \to 2^{\mathbb{R}}$, where $F_C(X) = \{ F(x) \mid x \in X \}$. That is, for a given set of elements X, $F_C(X)$ transforms every value $x \in X$ to F(x).

We want to show that $\forall a \in A_I$, $F_C(\gamma(a)) \subseteq \gamma(F^\#(a))$.

Fix $a \in A_I$ as an arbitrary interval, where $a = [x, y]$, $x \in \mathbb{R}$, $y \in \mathbb{R}$, and $x \leq y$.

Let γ convert a from an abstract interval $a = [x, y]$, to the set $\{ i \in \mathbb{R} \mid x \leq i, i \leq y \}$.

Since F is a monotonically increasing function, we know $\forall a_1 \in a$, $\forall a_2 \in a$, if $a_1 \leq a_2$, $F(a_1) \leq F(a_2)$

Then $\forall z \in \gamma(a)$, $F(x) \leq F(z) \leq F(y)$

Notice that $F_C(\gamma(a))$ forms the set $\{ F(i) \mid i \in \mathbb{R}, x \leq i, i \leq y \}$

Since $F^\#(a) = [F(x), F(y)]$, $\gamma(F^\#(a)$ forms the set $\{ i \in \mathbb{R} \mid F(x) \leq i, i \leq F(y) \}$

That is, $F_C(\gamma(a))$ applies F to all elements in the set of all elements in the interval (x, y).

Since F is monotonically increasing, we know that all elements in $F_C(\gamma(a))$ must be within the interval [F(x), F(y)].

$\gamma(F^{\#}(a))$ forms the set of all elements within the interval [F(x), F(y)].

Thus, $F_C(\gamma(a)) \subseteq \gamma(F^{\#}(a))$. Therefore, $F^{\#}(a)$ is sound.

In addition, since F is monotonically increasing, $\forall z \in \gamma(a)$, $F(x) \leq F(z) \leq F(y)$

This means the greatest lower bound of $F_C(\gamma(a))$ is F(x), and the lowest upper bound of $F_C(\gamma(a))$ is F(y). Therefore, a sound abstract transformer must, at the minimum, contain the interval [F(x), F(y)]

This means $\forall a \in A_I$, where a = (x, y), and for all sound abstract transformers $F^* : A_I \rightarrow A_I$, $\gamma(F^{\#}(a)) \subseteq F_C([x, y]) \subseteq \gamma(F^*(a))$.

Therefore, $F^{\#}(a)$ is both sound and the best possible interval abstract transformer, which is what we wanted to show.

6. Let $f : \mathbb{R} \cup \{-\infty, +\infty\} \to \mathbb{R} \cup \{-\infty, +\infty\}$ be defined as $f(x) = a \times x^2 + b \times x + c$, where $a, b, c \in \mathbb{R}$ are constants with $a \neq 0$. Write a sound and most precise interval abstract transformer $f^\sharp : A_I \to A_I$ for f, where A_I denotes the set of all intervals over the extended real numbers ($\mathbb{R} \cup \{-\infty, +\infty\}$). Additionally, formally prove the soundness of $f^\sharp$ and show that it is indeed the most precise interval transformer.
Hint: To prove soundness, first define the setwise concrete function $f_C : 2^{\mathbb{R}} \to 2^{\mathbb{R}}$ as $f_C(\mathscr{X}) = \{f(x) \mid x \in \mathscr{X}\}$, and then show that $\forall a \in A_I, f_C(\gamma(a)) \subseteq \gamma(f^\sharp(a))$. **[10 pts]**

A transformer $F^\#$ is sound if and only if $\forall z \in A$, $F(\gamma(z)) \subseteq_C \gamma(F^\#(z))$

A transformer $F^\#_{Best}$ is sound and best if for all other sound transformers, $F^\#$, $F^\#$ is not more precise than $F^\#_{Best}$. That is, $\forall z \in A$, $\gamma(F^\#_{Best}(z)) \subseteq_C \gamma(F^\#(z))$

$F(x) = a * x^2 + b * x + c$

Without loss of generality, assume that $a > 0$. We can see that F(x) forms a parabola with $F(-\infty) = F(\infty) = \infty$

Solving the derivative of F(x) gives $F'(x) = 2a * x + b = 0$, where $x = -b / 2a$. Call this constant M.

Since F(x) forms an upwards parabola, $(-\infty, M]$ must be monotone decreasing, and $[M, \infty)$ must be monotone increasing.

We can then define $F^\#$ as the following, $\forall d \in A_I$, $d = [x, y]$, $x \in \mathbb{R}$, $y \in \mathbb{R}$, $x \leq y$:

$F^\#([x, y]) = \{$

If $(x \leq M, y \leq M)$:

[F(y), F(x)]

If $(x \leq M, M \leq y)$:

[F(M), Max(F(x), F(y))]

If $(M \leq x, M \leq y)$:

[F(x), F(y)]

}

Since F(x) is monotone for the intervals $(-\infty, M]$ and $[M, \infty)$, when $[x, y] \subseteq (-\infty, M]$ or $[x, y] \subseteq [M, \infty)$, we can simply create a new interval based on the minimum and maximum values of F(x) and F(y).

Thus, if $M \notin d$, $F^\#(d) = [\text{Min}(F(x), F(y)), \text{Max}(F(x), F(y))]$

Since F(M) is an extrema, when $M \in d = [x, y]$, we know that $F(M) \in \gamma(F_C(d))$, and that $\forall z \in \gamma(F_C(d)), F(M) \leq z$.

Thus, if $M \in d$, $F^{\#}(d) = [F(M), Max(F(x), F(y))]$

Let $F_C : 2^{\mathbb{R}} \rightarrow 2^{\mathbb{R}}$, where $F_C(X) = \{ F(x) \mid x \in X \}$. That is, for a given set of elements X, $F_C(X)$ transforms every value $x \in X$ to F(x).

We want to show that $\forall a \in A_I$, $F_C(\gamma(a)) \subseteq \gamma(F^{\#}(a))$.

Fix $d \in A_I$ as an arbitrary interval, where $d = [x, y]$, $x \in \mathbb{R}$, $y \in \mathbb{R}$, and $x \leq y$.

Let γ convert d from an abstract interval $d = [x, y]$, to the set $\{ i \in \mathbb{R} \mid x \leq i, i \leq y \}$.

Notice that $F_C(\gamma(d))$ forms the set $\{ F(i) \mid i \in \mathbb{R}, x \leq i, i \leq y \}$

If $M \notin d$, then $F^{\#}(d) = [Min(F(x), F(y)), Max(F(x), F(y))]$, and $\gamma(F^{\#}(a)$ forms the set $\{ i \in \mathbb{R} \mid Min(F(x), F(y)) \leq i, i \leq Max(F(x), F(y)) \}$

If $M \in d = [x, y]$, then $F(M) \in \gamma(F_C(d))$, and $\forall z \in \gamma(F_C(d)), F(M) \leq z$.
Thus, if $M \in d$, $F^{\#}(d) = [F(M), Max(F(x), F(y))]$

This covers the entire interval of possible values for $F_C(\gamma(d))$.

Thus, $F_C(\gamma(d)) \subseteq \gamma(F^{\#}(d))$. Therefore, $F^{\#}(d)$ is sound.

In addition, we know F is monotonic for the intervals $(-\infty, M]$ and $[M, \infty)$.

If $M \notin d$, then the greatest lower bound of $F_C(\gamma(d))$ is Min(F(x), F(y)), and the lowest upper bound of $F_C(\gamma(d))$ is Max(F(x), F(y)). Therefore, if $M \notin d$, a sound abstract transformer must, at the minimum, contain the interval [Min(F(x), F(y)), Max(F(x), F(y))].

If $M \in d$, this means the greatest lower bound of $F_C(\gamma(a))$ is F(M), and the lowest upper bound of $F_C(\gamma(a))$ is Max(F(x), F(y)). Therefore, if $M \in d$, a sound abstract transformer must, at the minimum, contain the interval [F(M), Max(F(x), F(y))]

This means $\forall d \in A_I$, where d = (x, y), and for all sound abstract transformers F* : A_I -> A_I, $\gamma(F^{\#}(a)) \subseteq F_C([x, y]) \subseteq \gamma(F^*(a))$.

Therefore, $F^{\#}(a)$ is both sound and the best possible abstract interval transformer, which is what we wanted to show.

Reaching Definitions (20 pts)

7. Consider the following program defined over the variables `x, y, z`:

```
1  var x,y,z;
2  x = input;
3  while (x>1) {
4      z = x/2;
5      if (z>2) {
6          x = x+z;
7      }
8      y = x+2;
9      if (y>3) {
10         x = x/4;
11     }
12     z = z-4;
13 }
14 output z;
```

For each point in the program, determine a precise but sound approximation of the set of reaching definitions at that point. Show each iteration of the analysis at each point (Do not forget the entry and exit points).

Let the entry point of each iteration be the Reaching Definitions before a block of code is processed, and the exit point of each iteration be the Reaching Definitions after a block of code is processed.

Reaching Definitions at each line in the program, with loops:

```
L1:   var x, y, z;
L2:   x = input;                  #1
L3:   while (x > 1) {
L4:         z = x / 2             #2
            if (z > 2) {
L5:               x = x + 2;      #3
            }
L6:         y = x + 2;            #4
            if (y > 3) {
L7:               x = x / 4;      #5
            }
L8:         z = z - 4;            #6
      }
L9:   output z;
```

Let the indices in the numerical sequence "000000" correspond to the bit vectors for assigned definitions at positions #1, #2, #3, #4, #5, and #6. The indices correspond to the current line in the program that's being analyzed.

1. IN[1] = 000000, OUT[1] = 000000, GEN[1] = 000000, KILL[1] = 000000
2. IN[2] = 000000, OUT[2] = 100000, GEN[2] = 100000, KILL[2] = 000000
3. IN[3] = 100000, OUT[3] = 100000, GEN[3] = 000000, KILL[3] = 000000
4. IN[4] = 100000, OUT[4] = 110000, GEN[4] = 010000, KILL[4] = 000000
5. IN[5] = 110000, OUT[5] = 011000, GEN[5] = 001000, KILL[5] = 100000
6. IN[6] = 111000, OUT[6] = 111100, GEN[6] = 000100, KILL[6] = 000000
7. IN[7] = 111100, OUT[7] = 010110, GEN[7] = 000010, KILL[7] = 101000
8. IN[8] = 111110, OUT[8] = 101111, GEN[8] = 000001, KILL[8] = 010000
9. IN[3] = 101111, OUT[3] = 101111, GEN[3] = 000000, KILL[3] = 000000
10. IN[4] = 101111, OUT[4] = 111110, GEN[4] = 010000, KILL[4] = 000001
11. IN[5] = 111110, OUT[5] = 011100, GEN[5] = 001000, KILL[5] = 100010
12. IN[6] = 011100, OUT[6] = 111110, GEN[6] = 000100, KILL[6] = 000000
13. IN[7] = 111110, OUT[7] = 010110, GEN[7] = 000010, KILL[7] = 101000
14. IN[8] = 111110, OUT[8] = 101111, GEN[8] = 000001, KILL[8] = 010000
15. IN[3] = 101111, OUT[3] = 101111, GEN[3] = 000000, KILL[3] = 000000
16. IN[4] = 101111, OUT[4] = 111110, GEN[4] = 010000, KILL[4] = 000001
17. IN[5] = 111110, OUT[5] = 011100, GEN[5] = 001000, KILL[5] = 100010
18. IN[6] = 011100, OUT[6] = 111110, GEN[6] = 000100, KILL[6] = 000000
19. IN[7] = 111110, OUT[7] = 010110, GEN[7] = 000010, KILL[7] = 101000
20. IN[8] = 111110, OUT[8] = 101111, GEN[8] = 000001, KILL[8] = 010000
21. IN[9] = 101111, OUT[9] = 101111, GEN[9] = 000000, KILL[9] = 000000

No changes in iterations 14-20.