cs150: Exam 1

Due: Monday, 26 February at 12:02pm

Name:

Directions

Work alone. You may not discuss these problems or anything related to the material covered by this exam with anyone except for the course staff between receiving this exam and class Monday.

Open resources. You may use any books you want, lecture notes, slides, your notes, and problem sets. You may also use DrScheme, but it is not necessary to do this. You may also use external non-human sources including books and web sites. If you use anything other than the course books, slides, and notes, cite what you used. You may not obtain any help from other humans other than the course staff.

Answer well. Answer all questions 1-9 (question 0 is your name, which hopefully everyone will receive full credit for), and optionally answer questions 10-12.

You may either: (1) write your answers on this exam or (2) type and write your answers into the provided Word template (*/cs150/exams/exam1/exam1.doc*). Whichever you choose, you must turn in your answers printed on paper and they must be clear enough for us to read and understand. You should not need more space than is provided to write good answers, but if you want more space you may attach extra sheets. If you do, make sure the answers are clearly marked.

The questions are not necessarily in order of increasing difficulty, so if you get stuck on one question you should continue on to the next question. There is no time limit on this exam, but it should not take a well-prepared student more than a few hours to complete. It may take you longer, though, so please do not delay starting the exam. There is no valid excuse (other than a medical or personal emergency) for running out of time on this exam.

Full credit depends on the clarity and elegance of your answer, not just correctness. Your answers should be as short and simple as possible, but not simpler. Your programs will be judged for correctness, clarity and elegance, but you will not lose points for trivial errors (such as missing a closing parenthesis).

Scores

0	1	2	3	4	5	6	7	8	9	Total
10	10	10	10	10	10	10	10	10	10	100

1. The and-expression is a special form for logical conjunction. An and-expression has any number of operand expressions. For example, all of the expressions below are valid and-expressions (question 2 will describe the evaluation rule for and-expressions):

```
> (and)
#t
>(and (= 2 2) (= 3 3))
#t
>(and 3 6 2 5 3 #f 2 5 (car 3))
#f
```

Define a BNF grammar rule for the *AndExpression*. You may assume all the grammar rules from Chapter 3 are defined and use them in your answer.

2. For simplicity, the rest of this question assumes a limited version of the and expression that only takes two operands: `(and` $expr_1$ $expr_2$`)` This simplified and-expression behaves identically to the standard and-expression when applied to two operands, but is not defined for other than two operands. The evaluation rule for an and-expression is:

> To evaluate an and-expression, evaluate the first subexpression. If it evaluates to a false value, the value of the and-expression is false. Otherwise, the value of the and-expression is the value of the second subexpression.

Dana Carver doesn't like unnecessary special forms and suggest that the and special form can be replaced with this procedure:

```
(define (and e1 e2) (if e1 e2 #f))
```

Provide a convincing argument that the `and` procedure above is not equivalent to the and-expression special form. (Hint: describe inputs where they mean different things.)

For convenience, here is the find-maximum procedure from Chapter 4:

```
(define (find-maximum f low high)
    (if (= low high)
        (f low)
        (max (f low)
             (find-maximum f (+ low 1) high)))))
```

3. (This is a slight rewording of Question 2 of notes 5 and Exercise 4.8 in the book.) The `find-maximum` procedure we defined in Chapter 4 (and Notes 5) evaluates to the maximum value of the input function in the range, but does not provide the input value that produces that maximum output value. Define a procedure, `find-maximizing-input` that takes the same inputs as `find-maximum`, but outputs the input value in the range that produces the maximum output value.

For example:

```
> (find-maximizing-input (lambda (x) x) 3 150)
150
> (find-maximizing-input (lambda (x) (- (* 12 x) (* x x))) 0 50)
6
```

For maximum credit, your answer should have running time in $\Theta(n)$ where n is the difference between the values of the `high` and `low` inputs. (But you will receive most of the credit even if your solution is less efficient.)

4. Define a `make-incrementer` procedure that takes one input, the increment number, as input and produces as output a procedure. The output procedure is a procedure that takes one number as input, and produces as output the value of that number increased by the increment number.

For example:

```
> (make-incrementer 1)
#<procedure>
> ((make-incrementer 2) 148)
150
>((make-incrementer 3) ((make-incrementer 7) 1))
11
```

5. Define a procedure `find-worst` that takes two inputs: a list and a comparison procedure. As output it produces the element in the list which is the worst according to the comparison procedure.

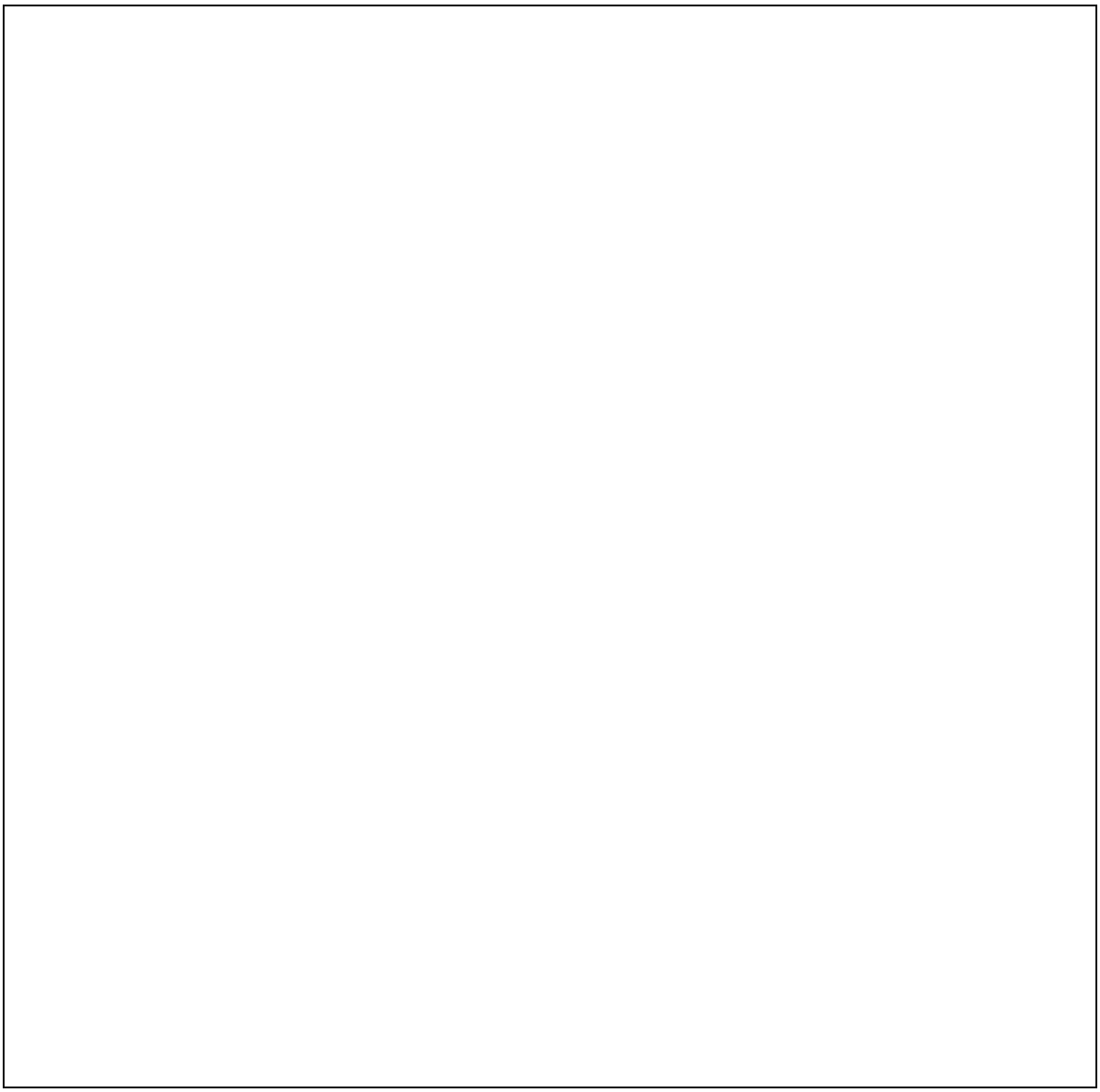
For example:

```
> (find-worst (list 1 5 0) <)
5
```

6. Draw a picture illustrating the asymptotic growth rates of the following functions and sets of functions:

a. $n^2 + 3n$
b. $O(2n)$
c. $\Theta(n)$
d. $\Omega(n^2)$

The center of your picture should be the slowest growing functions, and as you move further from the center, functions grow faster (similar to Figure 6.2 of the book). If you are depicting a set, use arrows or color to make it clear what space is included in the set. (There is no need for a fancy drawing. It is fine to hand draw something clear.)



Another cryptographic invention of Alan Turing's at Bletchley Park was a process then known as *banburismus* (more commonly now called *sequential analysis*) developed to determine if two intercepted Enigma messages had been encrypted using the same key.

The goal of the banburismus technique is to determine when two intercepted Enigma messages were encrypted using the same or similar initial machine settings. The key insight is identical to that behind the double delta technique used by Colossus: since the letter distribution in a natural language (in this cases German) is not even, it is much more likely that the same letters will occur at a given position than would occur by random chance (which is approximately the case if the Enigma machines were not configured with similar wheel settings).

So, to determine if two messages were sent by Enigma machines with the same wheel settings we need to count the number of occurrences in the ciphertext where the two messages have the same letter at the same position. If that number significantly exceeds the number predicted by random chance, then it is likely the messages were encoded using the same wheel settings.

7. Define a procedure `count-matches` that takes as input two lists of characters (representing two intercepted ciphertexts) and outputs a number that is the number of positions where the characters in the two lists match (use `eq?` to test two characters for equality).

For example,

```
> (count-matches (list #\A #\B #\C) (list #\B #\B #\C)
2
> (count-matches (list #\A #\B #\C) (list #\A))
1
>(count-matches (list #\A #\B #\C) (list #\A #\B #\C #\D))
3
```

Since the Enigma wheels rotate, it was also possible to use this technique to find messages sent using similar initial configurations by trying different alignments of the two messages. For example, suppose the intercepted messages are:

```
Message 1: GXCYBGDSLVWBDJLKWIPEHVYGQZWDTHRQXIKEESQSSPZXARIXEABQIRUCKHGWUEBPF
Message 2: YNSCFCCPVIPEMSGIZWFLHESCIYSPVRXMCFQAXVXDVUQILBJUABNLKMKDJMENUNQ
```

(this example is from http://en.wikipedia.org/wiki/Banburismus)

The Bletchley Park analysts would try aligning the messages at different starting points, looking for ways of aligning them that have a high number of matches. For example:

Align 0:

```
GXCYBGDSLVWBDJLKWIPEHVYGQZWDTHRQXIKEESQSSPZXARIXEABQIRUCKHGWUEBPF
YNSCFCCPVIPEMSGIZWFLHESCIYSPVRXMCFQAXVXDVUQILBJUABNLKMKDJMENUNQ
```

Align +1

```
GXCYBGDSLVWBDJLKWIPEHVYGQZWDTHRQXIKEESQSSPZXARIXEABQIRUCKHGWUEBPF
 YNSCFCCPVIPEMSGIZWFLHESCIYSPVRXMCFQAXVXDVUQILBJUABNLKMKDJMENUNQ
...
```

Align +9

```
GXCYBGDSLVWBDJLKWIPEHVYGQZWDTHRQXIKEESQSSPZXARIXEABQIRUCKHGWUEBPF
         YNSCFCCPVIPEMSGIZWFLHESCIYSPVRXMCFQAXVXDVUQILBJUABNLKMKDJMENUNQ
```

With the Align +9, there are 9 matches which is promising (that is, it would be very unlikely to occur by chance, so the wheel settings are probably similar).

8. Define a procedure `find-best-alignment` that takes as input two lists, representing two intercepted ciphertexts, and outputs the number of matching letters in the best possible alignment.

A good answer will find the best positive alignment (only considering moving the second message to the right, as in the example above). An excellent answer will consider both positive and negative alignments (moving the second message to the left instead).
For example:

```
> (find-best-alignment (list #\A #\B #\C) (list #\B #\B #\C))
2
> (find-best-alignment (list #\A #\B #\C #\D) (list #\B #\C #\D))
3
> (find-best-alignment (list #\A #\B #\C #\D)
                       (list #\F #\A #\B #\C #\D))
4
```

This is the correct result for "excellent" answers that consider negative alignments. The answer using just positive alignments is `0`.

Hint: note that the letters with no corresponding letter in the other message don't matter. So, we could view Align +1 above as

```
XCYBGDSLVWBDJLKWIPEHVYGQZWDTHRQXIKEESQSSPZXARIXEABQIRUCKHGWUEBPF
YNSCFCCPVIPEMSGIZWFLHESCIYSPVRXMCFQAXVXDVUQILBJUABNLKMKDJMENUNQ
```

without the leading `G` in message one.

(Answer space is on the next page)

8 (continued). Define your `find-best-alignment` procedure here:

9. Analyze the running time of your `find-best-alignment` procedure. Your analysis should include a description of the running time using Θ notation.

These three questions are optional and worth no credit, but we appreciate your answers. (Feel free to use as much space as you want to answer these.)

10. Do you feel your performance on this exam will fairly reflect your understanding of the course material so far? If not, explain why.

11. Do you have any comments about how the course is going so far or suggestions for improving the remainder of the course?

12. What topics do you hope to see in the remainder of the course?

End of Exam