Staff Solutions to Problem Set 4

Reading:
- Chapter 7. Recursive Data
- Chapter 8. Infinite Sets
- Chapter 9. Number Theory through 9.4. Fundamental Theorem of Arithmetic

Problem 1.
One way to determine if a string has matching brackets, that is, if it is in the set, RecMatch\(^1\), is to start with 0 and read the string from left to right, adding 1 to the count for each left bracket and subtracting 1 from the count for each right bracket. For example, here are the counts for two sample strings:

\[
\begin{array}{cccccccc}
0 & 1 & 0 & -1 & 0 & 1 & 2 & 3 & 4 & 3 & 2 & 1 & 0 \\
\end{array}
\]

\[
\begin{array}{cccccccc}
0 & 1 & 2 & 3 & 2 & 1 & 2 & 1 & 0 & 1 & 0 \\
\end{array}
\]

A string has a **good count** if its running count never goes negative and ends with 0. So the second string above has a good count, but the first one does not because its count went negative at the third step. Let

\[ \text{GoodCount} := \{ s \in \{ [], [ ]^* \} \mid s \text{ has a good count} \}. \]

The empty string has a length 0 running count we’ll take as a good count by convention, that is, \( \lambda \in \text{GoodCount} \). The matched strings can now be characterized precisely as this set of strings with good counts.

(a) Prove that GoodCount contains RecMatch by structural induction on the definition of RecMatch.

Solution. We prove by induction on the definition of RecMatch (that is, structural induction) that every element of RecMatch counts well, so RecMatch is contained in GoodCount. The induction hypothesis is

\[ P(s) := s \in \text{GoodCount}. \]

**Proof.** Base Case: \( P(\lambda) \) holds since the count of the empty string ends when it starts at zero.

Inductive Step: Assume \( P(s) \) and \( P(t) \) are true. We need to show that \( P([s]t) \) is true.

The count values for \([s]t\) start with 0. Reading the initial left bracket yields 1 as the next count value. This 1 serves as the start of a series of count values exactly equal to the count values of \( s \), with each value incremented by one. Since \( s \in \text{GoodCount} \) by hypothesis, these incremented count values begin with 1, always stay positive, and end with 1. The right bracket immediately after \( s \) reduces the ending count to 0. This 0 serves as the start of the remaining count values which are exactly the count values of \( t \). Since \( t \in \text{GoodCount} \), these remaining values never go negative and end at 0. Hence the entire sequence of count values for \([s]t\) starts with 0, never goes negative, and ends with 0, which proves that \([s]t \in \text{GoodCount}\).

---

\(^1\)RecMatch is defined recursively: **Base case**: \( \lambda \in \text{RecMatch} \). **Constructor case**: If \( s, t \in \text{RecMatch} \), then \([s]t \in \text{RecMatch}\).
(b) Conversely, prove that RecMatch contains GoodCount.

Hint: By induction on the length of strings in GoodCount. Consider when the running count equals 0 for the second time.

Solution. Proof. We show that every string \( r \in \text{GoodCount} \) is in RecMatch by strong induction on the length of \( r \). The induction hypothesis is

\[
Q(n) := \forall r \in \text{GoodCount}. |r| = n \implies r \in \text{RecMatch}.
\]

Base Case \( n = 0 \): In this case there is only one string of length \( n \), namely the empty string, which is in RecMatch by definition, proving \( Q(0) \).

Inductive Step: Assume that \( Q(k) \) is true for all \( k \leq n \), we need to prove that \( Q(n + 1) \) is also true.

So suppose \( r \) is a length \( n + 1 \) string that counts well. We must prove that \( r \in \text{RecMatch} \).

Now since \( r \) has a good count, it must start with a left bracket (or else the count would immediately go negative). Likewise, since the count for \( r \) returns to the value 0 by the end, \( r \) must end with right bracket. So there must be a first right bracket in \( r \) after which the count returns to 0. Let \( s \) be the substring of \( r \) between the initial left bracket and this right bracket. So

\[
r = [s]t
\]

for some string \( t \).

Since counts only change by one as each bracket character is read, and the count for \( r \) first returns to 0 after the right bracket following \( s \), the count during \( s \) must start and end with 1 and must stay positive in between. But this implies that a count for \( s \) alone, which would start with 0, would also end with 0 and stay nonnegative in between. That is, \( s \) by itself has a good count. Since the length of \( s \in \text{GoodCount} \) is less than the length of \( r \), we have by strong induction that \( s \in \text{RecMatch} \).

Further, we know the count for \( r \) returns to 0 after the right bracket following \( s \), and since \( r \in \text{GoodCount} \), the count ends with 0 again and stays nonnegative in between. But this implies that \( t \) has a good count, and since the length of \( t \) is less than the length of \( r \), we have by strong induction that \( t \in \text{RecMatch} \). Now by the second case in the definition of RecMatch, we conclude \( r = [s]t \in \text{RecMatch} \).

Problem 2.

Show that the set \( \mathbb{N}^* \) of finite sequences of nonnegative integers is countable.

Solution. Define the weight of a finite string of nonnegative integers to be the larger of the length of the string and the largest integer in the string. There are only finitely many strings of any given weight, \( n \), so list the strings in order of weight, ordered within same-weight groups in some arbitrary way, say in “dictionary” order.

Problem 3.

Let \( \mathbb{N}^{\omega} \) be the set of infinite sequences of nonnegative integers. For example, some sequences of this kind are:

\[
(0, 1, 2, 3, 4, \ldots),
(2, 3, 5, 7, 11, \ldots),
(3, 1, 4, 5, 9, \ldots).
\]

Prove that this set of sequences is uncountable.
Solution. Proof. One approach is to show that if \( \mathbb{N}^\omega \) were countable, then \( \text{pow}(\mathbb{N}) \) would be too, contradicting Cantor’s Theorem 8.1.11.

STAFF NOTE: If needed, offer hint: verify that \( \mathbb{N}^\omega \) is as big as \( \text{pow}(\mathbb{N}) \).

Namely, we can define a surjective function from \( f : \mathbb{N}^\omega \to \text{pow}(\mathbb{N}) \) as follows:

\[
f(s) := \{ n \in \mathbb{N} \mid s[n] = 0 \}
\]

where \( s[n] \) is the \( n \)th element of sequence \( s \).

Now if there was a surjective function from \( g : \mathbb{N} \to \mathbb{N}^\omega \), then the composition of \( f \) and \( g \) would be a surjective function from \( \mathbb{N} \) to \( \text{pow}(\mathbb{N}) \) contradicting Cantor’s Theorem 8.1.11.

Alternatively, to show that \( \mathbb{N}^\omega \) is uncountable, we can use a basic diagonal argument directly to show that no function from \( \mathbb{N} \) to the set of sequences \( \mathbb{N}^\omega \) is a surjection.

Proof. Let \( \sigma \) be a function from \( \mathbb{N} \) to the infinite sequences of nonnegative integers. To show that \( \sigma \) is not a surjection, we will describe a sequence, diag, of nonnegative integers that is not in the range of \( \sigma \).

Namely, define a sequence diag \( \in \mathbb{N}^\omega \) as follows:

STAFF NOTE: If needed, offer this def of diag as a hint.

\[
diag[n] := \sigma(n)[n] + 1.
\]

Now by definition,

\[
diag[n] \neq \sigma(n)[n],
\]

for all \( n \in \mathbb{N} \), proving that diag is not equal to \( \sigma(n) \) for any \( n \in \mathbb{N} \). This means that diag is not in the range of \( \sigma \), as claimed.

Problem 4.

Here is a game you can analyze with number theory and always beat me. We start with two distinct, positive integers written on a blackboard. Call them \( a \) and \( b \). Now we take turns. (I’ll let you decide who goes first.) On each turn, the player must write a new positive integer on the board that is the difference of two numbers that are already there. If a player cannot play, then they lose.

For example, suppose that 12 and 15 are on the board initially. Your first play must be 3, which is \( 15 - 12 \). Then I might play 9, which is \( 12 - 3 \). Then you might play 6, which is \( 15 - 9 \). Then I can’t play, so I lose.

(a) Show that every number on the board at the end of the game is a multiple of \( \gcd(a, b) \).

Solution. Thinking of the game as a state machine, we observe that the property that \( \gcd(a, b) \) divides all the numbers on the board is an invariant. This follows because the next state (board) is the same as the previous state, except for an additional number which is the difference of two numbers already there. Assuming these two numbers are divisible by \( \gcd(a, b) \), we know that their difference will be as well, which proves that the next state satisfies the invariant.

(b) Show that every positive multiple of \( \gcd(a, b) \) up to \( \max(a, b) \) is on the board at the end of the game.

Solution. Assume without loss of generality that \( a > b \). Let \( s \) be the smallest number on the board at the end of the game. So \( a = qs + r \) where \( 0 \leq r < s \) by the division algorithm. Then \( a - s \) must be on the board and thus so must \( a - 2s, a - 3s, \ldots, a - (q - 1)s \). However, \( r = a - qs \) cannot be on the board, since \( r < s \) and \( s \) is defined to be the smallest number there. The only explanation is that \( r = 0 \), which implies
that $s \mid a$. By the same argument, $s \mid b$. Therefore, $s$ is a common divisor of $a$ and $b$. Since $s$ is a multiple of the greatest common divisor of $a$ and $b$ by the preceding problem part, $s$ must actually be the greatest common divisor. We already argued that $a, a - s, a - 2s, \ldots, a - (q - 1)s$ must be on the board, and these are all the positive multiples of $\gcd(a, b)$ up to $\max(a, b)$.

\[ \square \]

(e) Describe a strategy that lets you win this game every time.

**Solution.** Assume without loss of generality that $a \geq b$. By the previous parts, the numbers that appear on the final board are precisely all the multiples $\leq a$ of $\gcd(a, b)$. Thus, for each game, we know exactly how many values will be placed on the board before the game ends. So if an odd number of values will appear on the final board (which happens precisely when $a$ is an even multiple of $\gcd(a, b)$), then choose to go first.

\[ \square \]

**Problem 5.**
The set of complex numbers that are equal to $m + n\sqrt{-5}$ for some integers $m, n$ is called $\mathbb{Z}[\sqrt{-5}]$. It will turn out that in $\mathbb{Z}[\sqrt{-5}]$, not all numbers have unique factorizations.

A sum or product of numbers in $\mathbb{Z}[\sqrt{-5}]$ is in $\mathbb{Z}[\sqrt{-5}]$, and since $\mathbb{Z}[\sqrt{-5}]$ is a subset of the complex numbers, all the usual rules for addition and multiplication are true for it. But some weird things do happen. For example, the prime 29 has factors:

(a) Find $x, y \in \mathbb{Z}[\sqrt{-5}]$ such that $xy = 29$ and $x \neq \pm 1 \neq y$.

**Solution.** Let $x = (3 + 2\sqrt{-5})$ and $y = (3 - 2\sqrt{-5})$, so

$$
(3 + 2\sqrt{-5})(3 - 2\sqrt{-5}) = 9 - 4 \cdot 5 = 9 + 5 \cdot 4 = 29.
$$

\[ \square \]

On the other hand, the number 3 is still a “prime” even in $\mathbb{Z}[\sqrt{-5}]$. More precisely, a number $p \in \mathbb{Z}[\sqrt{-5}]$ is called **irreducible** over $\mathbb{Z}[\sqrt{-5}]$ iff when $xy = p$ for some $x, y \in \mathbb{Z}[\sqrt{-5}]$, either $x = \pm 1$ or $y = \pm 1$.

**Claim.** The numbers $3, 2 + \sqrt{-5},$ and $2 - \sqrt{-5}$ are irreducible over $\mathbb{Z}[\sqrt{-5}]$.

In particular, this Claim implies that the number 9 factors into irreducibles over $\mathbb{Z}[\sqrt{-5}]$ in two different ways:

$$
3 \cdot 3 = (2 + \sqrt{-5})(2 - \sqrt{-5}).
$$

(1)

So $\mathbb{Z}[\sqrt{-5}]$ is an example of what is called a **non-unique factorization** domain.

To verify the Claim, we’ll appeal (without proof) to a familiar technical property of complex numbers given in the following Lemma.

**Definition.** For a complex number $c = r + si$ where $r, s \in \mathbb{R}$ and $i$ is $\sqrt{-1}$, the **norm**, $|c|$, of $c$ is $\sqrt{r^2 + s^2}$.

**Lemma.** For $c, d \in \mathbb{C}$,

$$
|cd| = |c||d|.
$$

(b) Prove that $|x|^2 \neq 3$ for all $x \in \mathbb{Z}[\sqrt{-5}]$.

**Solution.** Say $x = m + n\sqrt{-5}$ for $m, n \in \mathbb{Z}$. Now suppose to the contrary that $|x|^2 := m^2 + 5n^2 = 3$. But $m^2 + 5n^2 \geq 5$ for $n \neq 0$. Hence $n$ must be 0, in which case the integer $m$ must be $\pm \sqrt{3}$, a contradiction.

\[ \square \]

(c) Prove that if $x \in \mathbb{Z}[\sqrt{-5}]$ and $|x| = 1$, then $x = \pm 1$.
Solution. Proof. Say \( x = m + n \sqrt{-5} \) for \( m, n \in \mathbb{Z} \). So \( |x| = \sqrt{m^2 + 5n^2} \). But \( m^2 + 5n^2 > 1 \) if \( n \neq 0 \), so \( |x| = 1 \) implies \( \sqrt{m^2} = 1 \). That is, \( x = m = \pm 1 \).

(d) Prove that if \( |xy| = 3 \) for some \( x, y \in \mathbb{Z}[\sqrt{-5}] \), then \( x = \pm 1 \) or \( y = \pm 1 \).

Hint: \( |z|^2 \in \mathbb{N} \) for \( z \in \mathbb{Z}[\sqrt{-5}] \).

Solution. Proof.

\[
3 = |xy| \quad \text{implies} \quad 3^2 = |xy|^2 = |x|^2 |y|^2 \quad \text{(by the Lemma)} \\
\quad \text{implies} \quad |x|^2 = 1 \text{ OR } |y|^2 = 1 \text{ OR } |x|^2 = |y|^2 = 3 \quad \text{(by the hint and unique factorization of } 3^2 \text{ over } \mathbb{N}) \\
\quad \text{implies} \quad |x|^2 = 1 \text{ OR } |y|^2 = 3 \text{ OR } |y|^2 = 1 \\
\quad \text{implies} \quad |x|^2 = 1 \text{ OR } |y|^2 = 1 \quad \text{(by part (b))} \\
\quad \text{implies} \quad x = \pm 1 \text{ OR } y = \pm 1 \quad \text{(by part (c))}
\]

(e) Complete the proof of the Claim.

Solution. We must prove that \( 3 \), and \( 2 \pm \sqrt{-5} \) are irreducible over \( \mathbb{Z}[\sqrt{-5}] \). That is, suppose \( xy = 3 \), or \( xy = 2 \pm \sqrt{-5} \), for some \( x, y \in \mathbb{Z}[\sqrt{-5}] \). We must prove that either \( x = \pm 1 \) or \( y = \pm 1 \).

But by definition,

\[
|2 \pm \sqrt{-5}| = \sqrt{2^2 + 5 \cdot 1^2} = \sqrt{9} = 3 = |3|.
\]

So \( |xy| = 3 \) in any case, and part (d) implies \( x = \pm 1 \) or \( y = \pm 1 \), as required.