1. Axiomatic Systems

You're a military commander and your intelligence staff has intercepted some enemy communications. They've determined that all of the messages the enemy sends are strings in the set $\{+, -\}^*$. They've also gleaned that every message s that the enemy sends satisfies the following properties:

1. Every prefix of s has at least as many $+$ symbols as $-$ symbols.
2. Every suffix of s has at least as many $-$ symbols as $+$ symbols.

As part of your attempt to decipher your enemy's code, you decide it is worthwhile to try sending messages in their code to them. You therefore need to construct messages s, but you have to make sure that every message you can construct looks like an enemy message (satisfies the properties above). Moreover, you feel it is necessary to be able to construct every such message that the enemy could possible send.

Your task is to give a logical system, or a set of axioms and deduction rules, for messages with the two properties above. Prove that every message that your logical system can derive satisfies the two rules, and that every message that satisfies the two rules can be derived by your logical system. In other words, give a logic for this concept and prove its soundness and completeness.

Solution: Here is a logical system:

1. The empty string is a theorem (axiom).
2. If s is a theorem, then $+s-$ is a theorem.
3. If s_1 and s_2 are both theorems and non-empty strings, then $s_1 s_2$ is a theorem.

Soundness: We proceed by structural induction:

Base Case: The empty string trivially satisfies both properties because it has neither prefices nor suffices and hence it is a truth.

Inductive Hypothesis: Any theorem of length $\leq n$ is a truth.

Inductive Step: Let s be a theorem of length $n+1$. There are two ways we could have derived s. The first is that $s = +s'-$ for some string s' of length exactly $n-1$. By our inductive hypothesis s' is a truth, so that every prefix of s' has at least as many $+$ symbols as $-$ symbols and every suffix of s' has at least as many $-$ symbols as $+$ symbols. Every prefix of s, except for s itself, consists of a $+$ followed by some prefix of s'. Each of these prefices have at least as many $+$ as minus symbols. An analogous argument shows that, each suffix of s, excepting s itself, has at least as many $-$ symbols as $+$ symbols. Since s' is both a prefix and a suffix of s' it must be the case that it has the same number of $+$ and $-$ symbols. Therefore the string s also has the same number of $+$ and $-$ symbols. Combined with the arguments above, we see that s is a truth.

The second case is where $s = s_1 s_2$. Since both s_1 and s_2 are non-empty strings they both must have length $\leq n$. We can apply the inductive hypothesis to both of them. We will show that every prefix of s has at least as many + symbols as − symbols. An analogous argument will establish the other property. A prefix of s is either a prefix of s_1 or the entirety of s_1 concatenated with a prefix of s_2. In the first case the inductive hypothesis immediately reveals that this prefix satisfies the property in question. In the second case, the inductive hypothesis coupled with the fact that s_1 must have the same number of + and − symbols establishes the property. The same argument applied to suffices reveals that s is a truth.

Any theorem of length $n+1$ must be derived either by prepending a + symbol and appending − symbol, or by concatenating two strictly smaller strings. Thus our argument covers every theorem of length $n+1$. We have therefore established that every theorem of length $n+$ is also a truth. By induction we have shown that our system is sound.

Completeness: Again we proceed by structural induction.

Base Case: The only truth of length 0 is the empty string. It is the only string of length 0.

Inductive Hypothesis: All truths of length $\leq n$ are theorems.

Inductive Step: Consider a truth s of length $n+1$. Define a function $f_s(i)$ to be the number of + symbols in the first i characters minus the number of − symbols in the first i characters of s. Mathematically $f_s(i) = |\{j \in \{1, \ldots, i\} | s_j = +\}| - |\{j \in \{1, \ldots, i\} | s_j = -\}|$. Since s is a truth, $f_s(i) \geq 0 \forall i$ and $f_s(1) = 1$ and $f_s(n+1) = 0$. Either there is some $i^\star \leq n$ such that $f_s(i^\star) = 0$ or there f_s is strictly positive for $i \leq n$.

In the first case, define the two substrings $s' = s_1 \ldots s_{i^\star}$ and $s'' = s_{i^\star+1} \ldots s_{n+1}$ so that $s = s's''$. We will now argue that s' and s'' are truths. Since every prefix of s' is also a prefix of s and since s is a truth, every prefix of s' has at least as many + as − symbols. Since $f_s(i^\star) = 0$ we see that the number of + symbols in s' is equal to the number of − symbols. For the suffix beginning at index j, the prefix ending at index $j-1$ has at least as many + symbols as − symbols, but the entire string has the same number of + symbols as − symbols. This means that the suffix must have at least as many − symbols as + symbols. This holds true for all j so that s' is a truth. An analogous argument establishes that s'' is also a truth. Since s' and s'' are truths of length $\leq n$, by the inductive hypothesis we have that both are theorems. Consequently our logical system allows us to derive $s = s's''$ so that s is also a theorem.

In the second case, we have that $f_s(i) \geq 1$ for $1 \leq i \leq n$. Since $f_s(1) = 1$ and $f_s(n+1) = 0$ it is clear that the first character of s is a + symbol and the last character of s is a − symbol. We can therefore write $s = +s'-$, and we are left to show that s' is a truth. First, notice that $f_{s'}(i) \geq 0$ for all $i \leq n-1$ since $f_{s'}(i) = f_s(i+1) - 1$. In other words, the prefix of s' ending at the ith index has

exactly one fewer + symbol and the same number of − symbols as the analogous prefix of s (it is the prefix of length $i+1$ in s). Since every prefix of s of length $\leq n$ has strictly more + symbols than − symbols, we see that every prefix of s' has at least as many + symbols as − symbols. Thus s' satisfies the first property. Moreover, since $f_s(n+1) = 0$, we see that $f_{s'}(n-1) = 0$, or that s' has the same number of + and − symbols. The property about suffices follows from the same argument we used in the previous step: namely, if $f_{s'}(i) \geq 0$ then the suffix of s' starting at index $i+1$ must have at least as many − symbols as + symbols. Thus s' is a truth and by the inductive hypothesis it is also a theorem in our logical system. Consequently s is also a theorem, since it can be derived by rule 2.

In summary, we showed that every truth of length $n+1$ can either be derived by concatenating two theorems of smaller length, or by prepending a + and appending a − to a theorem of smaller length. We have therefore established that every truth of length $n+1$ is also a theorem. Consequently, our logical system is complete.

Notes: There are other possible solutions to this problem. For example the logical system with the empty string as an axiom and the deduction rule: "If x and y are truths then $x + -y$ is a truth." This logical system is both sound and complete.

2. Propositional Logic

(a) Let R, Q be propositional formulae. Describe a formula P that is a tautology iff R and Q are equisatisfiable.

Solution: Define P by $R \leftrightarrow Q$.

(b) Let $P_1, \ldots, P_k$ be a collection of propositional formulae. We say that this collection is consistent if there is a truth assignment which makes all P_i true. Write a formula S that is a tautology iff this collection is not consistent.

Solution: Let $S = \neg(P_1 \wedge P_2 \wedge \cdots \wedge P_k)$.

3. First-order Logic

Express each of the following predicates and propositions in first-order logic, where the universe is taken to be $\mathbb{N}$, the relations are $+(x, y, z)$, $*(x, y, z)$, and $=(x, y)$, where $+(x, y, z)$ is true iff $x + y = z$, and similarly for $*$, and there are no constants.

(a) n is the sum of two squares.

Solution: $\exists a \exists b \exists c \exists d (*(a, a, c) \wedge *(b, b, d) \wedge +(c, d, n))$.

(b) $n = 1$

Solution: $n = 1 \leftrightarrow *(n, n, n)$.

(c) m divides n ($m \mid n$).

Solution: $m \mid n \leftrightarrow \exists k(*(m, k, n))$.

(d) n is prime.

Solution: $isPrime(n) \leftrightarrow \forall k(k \mid n \rightarrow (k = 1 \vee = (k, n))$.

(e) n is a power of 2.

Solution:

$isPow2 \leftrightarrow \forall k((isPrime(k) \wedge k \mid n) \rightarrow (\exists m \exists a(a = 1 \wedge +(a, a, m) \wedge = (k, m)))$.