MATHEMATICS 300 — FALL 1998

Introduction to Mathematical Reasoning

Instructor: H. J. Sussmann

HANDOUT NO. 11. November 4, 1998

Revised and expanded, November 9, 1998. Revised again Nov. 16, 1998

NOTE: This is the second (and, I hope, final) version of this handout. The first version was just 6 pages. In this second version, the first 6 pages are still more or less the same as in the first version, except that I have corrected some typos, made a change in the list of problems for Homework No. 8, following what I said in class on November 4, and also made a few other changes.

CONTENTS

HOMEWORK ASSIGNMENT NO. 8, DUE ON MONDAY, NOVEMBER 16

1. Problems 8, 9, 10, 13, 14, and 15 in pages 94-95-96, nonstarred parts only, but do Problem 15(a) even though it is starred.

2. Problems 4(b), 5(b), (c), 6 (including part (d)), 12, and 15 in pages 102-103-104.

3. Prove or disprove: the product of 728 consecutive natural numbers is always divisible by 728!. (Recall: $n!$ is the *factorial* of n, defined inductively by $1! = 1$, $(n+1)! = (n+1).n!$ for $n \in \mathbb{N}$.)

4. Do problem 12 of page 72 using the rules of Handout 10, the definitions of $\subseteq$, $\cup$, $\cap$, $\emptyset$ and $=$ (given in the book) **and nothing else**. *(NOTE: this problem was originally part of homework assignment No. 7, due on November 4. On November 4, I announced in class that (a) the deadline for homework assignment No. 7 was extended to November 9, and (b) this particular problem, which was No. 3 of homework assignment No. 7, was now moved to homework assignment No. 8.)*

TYPOS IN HANDOUT NO. 10

Please correct the following two typos in Handout No. 10 (revised version):

- In page 1, line 5, where it says "Revised November 22, 1998," it should say "Revised November 2, 1998."
- In page 10, line 3, where it says "Rule 3 or Rule 4 or Rule 5," it should say "Rule 3 or Rule 5 or Rule 6."

TYPOS IN THE BOOK

- In page 86, line 5 (right below statement (ii)), where it says "$S \in \mathbb{N}$" it should say "$S = \mathbb{N}$."
- In page 88, box, the title should be "PROOF OF $(\forall n \in \mathbb{N})P(n)$ BY INDUCTION" rather than "PROOF OF $(\forall x \in \mathbb{N})P(n)$ BY INDUCTION."
- In page 88, box, the "basic step" should be "Show that $P(1)$ is true" rather than "Show that $1 \in S$."
- In page 103, 2nd line of part (d) of problem 6, where it says "$\alpha = \frac{1-\sqrt{5}}{2}$," it should say "$\beta = \frac{1-\sqrt{5}}{2}$."

READING FOR NOVEMBER 9 AND 11

- Book, sections 2.4 and 2.5.
- Handouts No. 10 and 11.

SOME EXAMPLES OF PROOFS IN "PURE LOGIC"

Let $p(x)$ be a formula that has no quantifiers in x and has no free variables other than x.

THEOREM I. $(\exists x)p(x) \Leftrightarrow (\sim (\forall x)(\sim p(x)))$.

INFORMAL PROOF: Suppose that $(\exists x)p(x)$. Let us show that $\sim (\forall x)(\sim p(x))$ by contradiction. Assume $(\forall x)(\sim p(x))$. Pick an a such that $p(a)$, which is possible because we are assuming that such an a exists. Since $(\forall x)(\sim p(x))$, we get $\sim p(a)$, contradicting the fact that $p(a)$. Therefore the assumption that $(\forall x)(\sim p(x))$ leads to a contradiction. So $\sim (\forall x)(\sim p(x))$, as desired.

Now suppose that $\sim (\exists x)p(x)$. Let us show that $(\forall x)(\sim p(x))$. Pick an arbitrary a. We want to prove that $\sim p(a)$. Suppose this was false, i.e. suppose that $p(a)$. Then it would follow that $(\exists x)p(x)$, contradictiong our assumption that $\sim (\exists x)p(x)$. So $p(a)$ leads to a contradiction. Therefore $\sim p(a)$. Since a was arbitrary, we have established that $(\forall x)(\sim p(x))$, as desired.

So we have shown that $(\exists x)p(x)$ implies $\sim (\forall x)(\sim p(x))$, and also that $\sim (\exists x)p(x)$ implies $(\forall x)(\sim p(x))$. Therefore $(\exists x)p(x) \Leftrightarrow (\sim (\forall x)(\sim p(x)))$. **QED**

FORMAL PROOF:

(1.&)	Assume $(\exists x)p(x)$.	[Preparation to apply Rule 3]
(2.&.&)	Let a be such that $p(a)$.	[From (1), preparation to apply Rule 6]
(3.&.&.&)	Assume $(\forall x)(\sim p(x))$.	[Preparation to apply Rule 3]
(4.&.&.&)	$\sim p(a)$.	[Rule 4, from (3)]
(5.&.&.&)	$(\sim p(a)) \Rightarrow (p(a) \Rightarrow (\sim (\forall x)(\sim p(x))))$.	[Tautology $(\sim \alpha) \Rightarrow (\alpha \Rightarrow \beta)$]
(6.&.&.&)	$p(a) \Rightarrow (\sim (\forall x)(\sim p(x)))$.	[Modus Ponens from (4) and (5)]
(7.&.&.&)	$\sim (\forall x)(\sim p(x))$.	[Modus Ponens from (2) and (6)]
(8.&.&)	$(\forall x)(\sim p(x)) \Rightarrow (\sim (\forall x)(\sim p(x)))$.	[Rule 3, from (3) and (7)]
(9.&.&)	$((\forall x)(\sim p(x)) \Rightarrow (\sim (\forall x)(\sim p(x)))) \Rightarrow (\sim (\forall x)(\sim p(x)))$.	[Tautology $(\alpha \Rightarrow (\sim \alpha)) \Rightarrow (\sim \alpha)$]
(10.&.&)	$\sim (\forall x)(\sim p(x))$.	[Modus Ponens, from (8) and (9)]
(11.&)	$\sim (\forall x)(\sim p(x))$.	[Rule 6, from (2) and (10)]
(12)	$(\exists x)p(x) \Rightarrow (\sim (\forall x)(\sim p(x)))$.	[Rule 3, from (1) and (11)]
(13.&)	Assume $\sim (\exists x)p(x)$.	[Preparation to apply Rule 3]
(14.&.&)	Let a be arbitrary.	[Preparation to apply Rule 5]
(15.&.&.&)	Assume $p(a)$.	[Preparation to apply Rule 3]
(16.&.&.&)	$(\exists x)p(x)$.	[Rule 7, from (15)]
(17.&.&.&)	$((\sim \exists x)p(x)) \Rightarrow ((\exists x)p(x) \Rightarrow (\sim p(a)))$.	[Tautology $(\sim \alpha) \Rightarrow (\alpha \Rightarrow \beta)$]
(18.&.&.&)	$(\exists x)p(x) \Rightarrow (\sim p(a))$.	[Modus Ponens from (13) and (17)]
(19.&.&.&)	$\sim p(a)$.	[Modus Ponens from (16) and (18)]
(20.&.&)	$p(a) \Rightarrow (\sim p(a))$.	[Rule 3, from (15) and (19)]
(21.&.&)	$(p(a) \Rightarrow (\sim p(a))) \Rightarrow (\sim p(a))$.	[Tautology $(\alpha \Rightarrow (\sim \alpha)) \Rightarrow (\sim \alpha)$]
(22.&.&)	$\sim p(a)$.	[Modus Ponens from (20) and (21)]
(23.&)	$(\forall x)(\sim p(x))$.	[Rule 5, from (14) and (22)]
(24)	$(\sim (\exists x)p(x)) \Rightarrow (\forall x)(\sim p(x))$.	[Rule 3, from (13) and (23)]
(25)	$((\exists x)p(x) \Rightarrow (\sim (\forall x)(\sim p(x)))) \Rightarrow$ $(((\sim (\exists x)p(x)) \Rightarrow (\forall x)(\sim p(x))) \Rightarrow ((\exists x)p(x) \Leftrightarrow (\sim (\forall x)(\sim p(x)))))$.	[Tautology $(\alpha \Rightarrow (\sim \beta)) \Rightarrow (((\sim \alpha) \Rightarrow \beta) \Rightarrow (\alpha \Leftrightarrow (\sim \beta)))$]
(26)	$((\sim (\exists x)p(x)) \Rightarrow (\forall x)(\sim p(x))) \Rightarrow ((\exists x)p(x) \Leftrightarrow (\sim (\forall x)(\sim p(x))))$.	[Modus Ponens from (12) and (25)]
(27)	$(\exists x)p(x) \Leftrightarrow (\sim (\forall x)(\sim p(x)))$.	[Modus Ponens from (24) and (26)]

QED

Read the above proofs carefully, and make sure you see that the "informal proof" and the "formal proof" really say the same thing. The formal proof is the detailed execution of the outline given in the informal proof. The informal proof can be thought of as an abbreviated narrative describing, or outlining, the formal proof.

ANOTHER "PURE LOGIC" EXAMPLE

Let $p(x)$, $q(x)$ be formulas having no quantifiers in x and having no free variables other than x.

THEOREM II. $(\forall x)(p(x) \wedge q(x)) \Leftrightarrow ((\forall x)p(x) \wedge (\forall x)q(x))$.

INFORMAL PROOF: Suppose $(\forall x)(p(x) \wedge q(x))$. We prove that $(\forall x)p(x) \wedge (\forall x)q(x)$. Pick an arbitrary a. Then $p(a) \wedge q(a)$. So, in particular, $p(a)$, and, since a was arbitrary, we have shown that $(\forall x)p(x)$. A similar argument shows that $(\forall x)q(x)$. So $(\forall x)p(x) \wedge (\forall x)q(x)$, as desired.

We now prove the converse. Suppose that $(\forall x)p(x) \wedge (\forall x)q(x)$. We prove that $(\forall x)(p(x) \wedge q(x))$. Let a be arbitrary. Since we are assuming that $(\forall x)p(x) \wedge (\forall x)q(x)$, it follows in particular that $(\forall x)p(x)$, so $p(a)$ holds, by specialization. A smilar argument shows that $q(a)$ holds. So $p(a) \wedge q(a)$. Since a was arbitrary, we have shown that $(\forall x)(p(x) \wedge q(x))$, as desired. **QED**

FORMAL PROOF:

(1.&)	Assume $(\forall x)(p(x) \wedge q(x))$.	[Preparation to apply Rule 3]
(2.&.&)	Let a be arbitrary.	[Preparation to apply Rule 5]
(3.&.&)	$p(a) \wedge q(a)$.	[Rule 4, from (1)]
(4.&.&)	$(p(a) \wedge q(a)) \Rightarrow p(a)$	[Tautology $(\alpha \wedge \beta) \Rightarrow \alpha$]
(5.&.&)	$p(a)$.	[Modus Ponens from (3) and (4)]
(6.&)	$(\forall x)p(x)$.	[Rule 5, from (2) and (5)]
(7.&.&)	Let a be arbitrary.	[Preparation to apply Rule 5]
(8.&.&)	$p(a) \wedge q(a)$.	[Rule 4, from (1)]
(9.&.&)	$(p(a) \wedge q(a)) \Rightarrow q(a)$.	[Tautology $(\alpha \wedge \beta) \Rightarrow \beta$]
(10.&.&)	$q(a)$.	[Modus Ponens from (8) and (9)]
(11.&)	$(\forall x)q(x)$.	[Rule 5, from (7) and (10)]
(12.&)	$(\forall x)p(x) \Rightarrow ((\forall x)q(x) \Rightarrow ((\forall x)p(x) \wedge (\forall x)q(x)))$.	[Tautology $\alpha \Rightarrow (\beta \Rightarrow (\alpha \wedge \beta))$]
(13.&)	$(\forall x)q(x) \Rightarrow ((\forall x)p(x) \wedge (\forall x)q(x))$.	[Modus Ponens from (6) and (12)]
(14.&)	$(\forall x)p(x) \wedge (\forall x)q(x)$.	[Modus Ponens from (11) and (13)]
(15)	$(\forall x)(p(x) \wedge q(x)) \Rightarrow ((\forall x)p(x) \wedge (\forall x)q(x))$.	[Rule 3, from (1) and (14)]
(16.&)	Assume $(\forall x)p(x) \wedge (\forall x)q(x)$.	[Preparation to apply Rule 3]
(17.&)	$((\forall x)p(x) \wedge (\forall x)q(x)) \Rightarrow (\forall x)p(x)$.	[Tautology $(\alpha \wedge \beta) \Rightarrow \alpha$]
(18.&)	$(\forall x)p(x)$.	[Modus Ponens from (16) and (17)]
(19.&)	$((\forall x)p(x) \wedge (\forall x)q(x)) \Rightarrow (\forall x)q(x)$.	[Tautology $(\alpha \wedge \beta) \Rightarrow \beta$]
(20.&)	$(\forall x)q(x)$.	[Modus Ponens from (16) and (19)]
(21.&.&)	Let a be arbitrary.	[Preparation to apply Rule 5]
(22.&.&)	$p(a)$.	[Rule 4, from (18)]
(23.&.&)	$q(a)$.	[Rule 4, from (20)]
(24.&.&)	$p(a) \Rightarrow (q(a) \Rightarrow (p(a) \wedge q(a)))$.	[Tautology $\alpha \Rightarrow (\beta \Rightarrow (\alpha \wedge \beta))$]
(25.&.&)	$q(a) \Rightarrow (p(a) \wedge q(a))$.	[Modus Ponens from (22) and (24)]
(26.&.&)	$p(a) \wedge q(a)$.	[Modus Ponens from (23) and (25)]
(27.&)	$(\forall x)(p(x) \wedge q(x))$.	[Rule 5, from (21) and (26)]
(28)	$((\forall x)p(x) \wedge (\forall x)q(x)) \Rightarrow (\forall x)(p(x) \wedge q(x))$.	[Rule 3, from (16) and (27)]
(29)	$((\forall x)(p(x) \wedge q(x)) \Rightarrow ((\forall x)p(x) \wedge (\forall x)q(x)))$ $\Rightarrow ((((\forall x)p(x) \wedge (\forall x)q(x)) \Rightarrow (\forall x)(p(x) \wedge q(x)))$ $\Rightarrow ((\forall x)(p(x) \wedge q(x)) \Leftrightarrow ((\forall x)p(x) \wedge (\forall x)q(x))))$.	[Tautology $(\alpha \Rightarrow \beta) \Rightarrow ((\beta \Rightarrow \alpha) \Rightarrow (\alpha \Leftrightarrow \beta))$]
(30)	$(((\forall x)p(x) \wedge (\forall x)q(x)) \Rightarrow (\forall x)(p(x) \wedge q(x)))$ $\Rightarrow ((\forall x)(p(x) \wedge q(x)) \Leftrightarrow ((\forall x)p(x) \wedge (\forall x)q(x)))$.	[Modus Ponens, from (15) and (29)]
(31)	$(\forall x)(p(x) \wedge q(x)) \Leftrightarrow ((\forall x)p(x) \wedge (\forall x)q(x))$.	[Modus Ponens, from (28) and (30)]

QED

Once again, you should read the above proofs carefully, and make sure you see that the "informal proof" and the "formal proof" really say the same thing. The formal proof is the detailed execution of the outline given in the informal proof. The informal proof can be thought of as an abbreviated narrative describing, or outlining, the formal proof.

QUESTION: Can you prove using the same technique that

$$(\forall x)(p(x) \vee q(x)) \Leftrightarrow ((\forall x)p(x) \vee (\forall x)q(x)) \ ?$$

TWO MORE EXAMPLES OF "PURE LOGIC" PROOFS

Let $q(x)$ be a formula having no quantifiers in x and having no free variables other than x, and let r be a sentence (that is, a formula without any open variables).

THEOREM III: $(\exists x)(r \wedge q(x)) \Rightarrow (r \wedge (\exists x)q(x))$.

THEOREM IV: $(\forall x)(r \vee q(x)) \Rightarrow (r \vee (\forall x)q(x))$.

INFORMAL PROOF OF THEOREM III: Suppose $(\exists x)(r \wedge q(x))$. We will prove that $r \wedge (\exists x)q(x)$. Pick a such that $r \wedge q(a)$. Then r and $q(a)$ hold. Since $q(a)$ is true, we have $(\exists x)q(x)$. Since we also have r, we can conclude that $r \wedge (\exists x)q(x)$.

Now let us prove the converse. Assume that $r \wedge (\exists x)q(x)$. We will prove that $(\exists x)(r \wedge q(x))$. Since $r \wedge (\exists x)q(x)$, it follows that both r and $(\exists x)q(x)$ hold. Pick a such that $q(a)$. Then r and $q(a)$ are true, so $r \wedge q(a)$ is true. Therefore $(\exists x)(r \wedge q(x))$. **QED**

FORMAL PROOF OF THEOREM III:

(1.&)	Assume $(\exists x)(r \wedge q(x))$.	[Preparation to apply Rule 3]
(2.&.&)	Let a be such that $r \wedge q(a)$.	[Rule 6, from (1)]
(3.&.&)	$(r \wedge q(a)) \Rightarrow r$	[Tautology $(\alpha \wedge \beta) \Rightarrow \alpha$]
(4.&.&)	$(r \wedge q(a)) \Rightarrow q(a)$	[Tautology $(\alpha \wedge \beta) \Rightarrow \beta$]
(5.&.&)	r.	[Modus Ponens, from (2) and (3)]
(6.&.&)	$q(a)$.	[Modus Ponens, from (2) and (4)]
(7.&.&)	$(\exists x)q(x)$.	[Rule 7, from (6)]
(8.&.&)	$r \Rightarrow ((\exists x)q(x) \Rightarrow (r \wedge (\exists x)q(x)))$.	[Tautology $\alpha \Rightarrow (\beta \Rightarrow (\alpha \wedge \beta))$]
(9.&.&)	$(\exists x)q(x) \Rightarrow (r \wedge (\exists x)q(x))$.	[Modus Ponens, from (5) and (8)]
(10.&.&)	$r \wedge (\exists x)q(x)$.	[Modus Ponens, from (7) and (9)]
(11.&)	$r \wedge (\exists x)q(x)$.	[Rule 6, from (2) and (10)]
(12)	$(\exists x)(r \wedge q(x)) \Rightarrow (r \wedge (\exists x)q(x))$.	[Rule 3, from (1) and (11)]
(13.&)	Assume $r \wedge (\exists x)q(x)$.	[Preparation to apply Rule 3]
(14.&)	$(r \wedge (\exists x)q(x)) \Rightarrow r$.	[Tautology $(\alpha \wedge \beta) \Rightarrow \alpha$]
(15.&)	$(r \wedge (\exists x)q(x)) \Rightarrow (\exists x)q(x)$.	[Tautology $(\alpha \wedge \beta) \Rightarrow \beta$]
(16.&)	r.	[Modus Ponens, from (13) and (14)]
(17.&)	$(\exists x)q(x)$.	[Modus Ponens, from (13) and (15)]
(18.&.&)	Let a be such that $q(a)$.	[Rule 6, from (17)]
(19.&.&)	$r \Rightarrow (q(a) \Rightarrow (r \wedge q(a)))$.	[Tautology $\alpha \Rightarrow (\beta \Rightarrow (\alpha \wedge \beta))$]
(20.&.&)	$q(a) \Rightarrow (r \wedge q(a))$.	[Modus Ponens, from (16) and (19)]
(21.&.&)	$r \wedge q(a)$.	[Modus Ponens, from (18) and (20)]
(22.&.&)	$(\exists x)(r \wedge q(x))$.	[Rule 7, from (21)]
(23.&)	$(\exists x)(r \wedge q(x))$.	[Rule 6, from (18) and (22)]
(24)	$(r \wedge (\exists x)q(x)) \Rightarrow (\exists x)(r \wedge q(x))$.	[Rule 3, from (13) and (23)]

Now let us write A and B as abbreviations for $(\exists x)(r \wedge q(x))$ and $r \wedge (\exists x)q(x)$, respectively.

(25)	$(A \Rightarrow B) \Rightarrow ((B \Rightarrow A) \Rightarrow (A \Leftrightarrow B))$.	[Tautology]
(26)	$(B \Rightarrow A) \Rightarrow (A \Leftrightarrow B)$.	[Modus Ponens, from (12)—which says $A \Rightarrow B$—and (25)]
(27)	$A \Leftrightarrow B$.	[Modus Ponens, from (24)—which says $B \Rightarrow A$—and (26)]

QED

INFORMAL PROOF OF THEOREM IV: Suppose $(\forall x)(r \vee q(x))$. We will prove that $r \vee (\forall x)q(x)$. We consider two cases: Case 1 is when r is true, and Case 2 is when r is false. In Case 1, r holds, so $r \vee (\forall x)q(x)$ holds as well. Now consider Case 2, that is, suppose r is not true. Let a be arbitrary. Since $(\forall x)(r \vee q(x))$, we can conclude that $r \vee q(a)$. Since r is not true, $q(a)$ must hold. But a is arbitrary, so $(\forall x)q(x)$ is true, and then $r \vee (\forall x)q(x)$ is also true. So we have shown that $r \vee (\forall x)q(x)$ holds in both cases.

Now let us prove the converse. Assume that $r \vee (\forall x)q(x)$. We will prove that $(\forall x)(r \vee q(x))$. Let a be arbitrary. We want to prove that $r \vee q(a)$. Since $r \vee (\forall x)q(x)$, it follows that either r or $(\forall x)q(x)$ is true. If r is true, then $r \vee q(a)$ is true, and we are done. If $(\forall x)q(x)$ is true, then we can specialize and conclude that $q(a)$ is true, so $r \vee q(a)$ is true as well. So we have shown that $r \vee q(a)$ is true in both cases. Since a was arbitrary, we have proved that $(\forall x)(r \vee q(x))$. **QED**

FORMAL PROOF OF THEOREM IV:

(1.&)	Assume $(\forall x)(r \vee q(x))$.	[Preparation to apply Rule 3]
(2.&.&)	Assume $\sim r$.	[Preparation to apply Rule 3]
(3.&.&.&)	Let a be arbitrary.	[Preparation to apply Rule 5]
(4.&.&.&)	$r \vee q(a)$.	[Rule 4, from (1)]
(5.&.&.&)	$(\sim r) \Rightarrow ((r \vee q(a)) \Rightarrow q(a))$.	[Tautology $(\sim \alpha) \Rightarrow ((\alpha \vee \beta) \Rightarrow \beta)$]
(6.&.&.&)	$(r \vee q(a)) \Rightarrow q(a)$.	[Modus Ponens from (2) and (5)]
(7.&.&.&)	$q(a)$.	[Modus Ponens from (4) and (6)]
(8.&.&)	$(\forall x)q(x)$.	[Rule 5, from (3) and (7)]
(9.&)	$(\sim r) \Rightarrow (\forall x)q(x)$.	[Rule 3, from (2) and (8)]
(10.&)	$((\sim r) \Rightarrow (\forall x)q(x)) \Rightarrow (r \vee (\forall x)q(x))$.	[Tautology $((\sim \alpha) \Rightarrow \beta) \Rightarrow (\alpha \vee \beta)$]
(11.&)	$r \vee (\forall x)q(x)$.	[Modus Ponens from (9) and (10)]
(12)	$(\forall x)(r \vee q(x)) \Rightarrow (r \vee (\forall x)q(x))$.	[Rule 3 from (1) and (11)]
(13.&)	Assume $r \vee (\forall x)q(x)$.	[Preparation to apply Rule 3]
(14.&.&)	Let a be arbitrary.	[Preparation to apply Rule 5]
(15.&.&.&)	Assume $\sim r$.	[Preparation to apply Rule 3]
(16.&.&.&)	$(\sim r) \Rightarrow ((r \vee (\forall x)q(x)) \Rightarrow (\forall x)q(x))$.	[Tautology $(\sim \alpha) \Rightarrow ((\alpha \vee \beta) \Rightarrow \beta)$]
(17.&.&.&)	$(r \vee (\forall x)q(x)) \Rightarrow (\forall x)q(x)$.	[Modus Ponens from (15) and (16)]
(18.&.&.&)	$(\forall x)q(x)$.	[Modus Ponens from (11) and (17)]
(19.&.&.&)	$q(a)$.	[Rule 4, from (18)]
(20.&.&)	$(\sim r) \Rightarrow q(a)$.	[Rule 3, from (15) and (18)]
(21.&.&)	$((\sim r) \Rightarrow q(a)) \Rightarrow (r \vee q(a))$.	[Tautology $((\sim \alpha) \Rightarrow \beta) \Rightarrow (\alpha \vee \beta)$]
(22.&.&)	$r \vee q(a)$.	[Modus Ponens from (2) and (21)]
(23.&)	$(\forall x)(r \vee q(x))$.	[Rule 5, from (14) and (22)]
(24)	$(r \vee (\forall x)q(x)) \Rightarrow (\forall x)(r \vee q(x))$.	[Rule 3, from (13) and (23)]

Now let us write A, B as abbreviations for $(\forall x)(r \vee q(x))$ and $r \vee (\forall x)q(x)$, respectively.

(25)	$(A \Rightarrow B) \Rightarrow ((B \Rightarrow A) \Rightarrow (A \Leftrightarrow B))$.	[Tautology]
(26)	$(B \Rightarrow A) \Rightarrow (A \Leftrightarrow B)$.	[Modus Ponens, from (12)—which says $A \Rightarrow B$—and (26)]
(27)	$A \Leftrightarrow B$.	[Modus Ponens, from (24)—which says $B \Rightarrow A$—and (25)]

QED

AXIOMS FOR EQUALITY

A **predicate calculus with equality** contains the binary function symbol $=$. If t, s are terms, We write $t = s$ rather than $= (t, s)$.
The following three **axioms** are automatically adopted in a predicate calculus with equality.

(EQ.1) $(\forall x)(x = x)$.

(EQ.2) $(\forall x)(\forall y)(x = y \Rightarrow y = x)$.

(EQ.3) $(\forall x)(\forall y)(\forall z)((x = y \wedge y = z) \Rightarrow x = z)$.

ABBREVIATIONS

Often, we end up writing formnulas that are too long. So it is convenient to introduce **abbreviations**. For example, suppose we are working with a predicate calculus with equality. We would like to introduce the symbol $\neq$ to stand for "not equal to," so that, for example, instead of writing "$\sim 3 = 5$," we would write "$3 \neq 5$."

One possibility would be to think of $\neq$ as a symbol of the given language. In that case, if we want $\neq$ to have its true meaning, we would have to include an **axiom** for it, for example:

$$(\forall x)(\forall y)(x \neq y \Leftrightarrow (\sim x = y))\,.$$

Another possibility would be to think of an expression such as $3 \neq 5$ as an abbreviation of $\sim 3 = 5$. With this interpretation, we would think that $\neq$ is **not** a symbol of our language, and that when we write $3 \neq 5$ this is just a "name," or abbreviation, for the formula $\sim 3 = 5$.

We will use the "axiom" approach in some cases, and the "abbreviation" approach in others. A detailed discussion of these two approaches and their pros and cons will be given later.

THE ABBREVIATIONS $\neq$ and $\exists!$

In a first-order predicate calculus with equality, we introduce the abbreviation $\neq$ to stand for "not equal to." Precisely:

ABBR.1: If t and s are terms, then "$t \neq s$" is an abbreviation of "$\sim t = s$."

Also, we will use $\exists!$ as an abbreviation for "there is one and only one." Precisely:

ABBR.2: If $p(x)$ is a formula not containing the variable y, then "$(\exists! x)p(x)$" is an abbreviation of "$(\exists x)(p(x) \wedge (\forall y)(p(y) \Rightarrow y = x))$."

USING ABBREVIATIONS

When we have abbreviations, we need **rules** telling us how to work with them. There are two such rules:

EXPAND: If A is an abbreviation for B, then we can write B wherever we have A.

ABBREVIATE: If A is an abbreviation for B, then we can write A wherever we have B.

For example: suppose that at some point we have arrived at

(35) $(\exists x)((x.x = 2 \wedge x \geq 0) \wedge (\forall y)((y.y = 2 \wedge y \geq 0) \Rightarrow y = x))\,.$ [...]

Then we can write:

(36) $(\exists! x)(x.x = 2 \wedge x \geq 0)\,.$ [Abbreviate (35); ABBR.2]

Conversely, if at some point we have

(87) $(\exists! x)(x.x = 2 \wedge x \geq 0)\,,$ [...]

then we can write:

(88) $(\exists x)((x.x=2 \wedge x \geq 0) \wedge (\forall y)((y.y=2 \wedge y \geq 0) \Rightarrow y=x))$. [Expand (87); ABBR.2]

SET THEORY

In **Set Theory**, we use a first-order predicate calculus with equality, containing the binary predicate symbols $=$ and $\in$ and the reserved constant[1] $\emptyset$.

The symbol $\emptyset$ is supposed to denote "the empty set." The symbol $\in$ is thought of as saying "belongs to," and written between its two arguments. So we write "$x \in y$" rather than "$\in (x, y)$," exactly as in arithmetic we write "$x < y$" rather than "$< (x, y)$." Naturally, the $=$ symbol is also written in the middle. The three axioms for equality hold.

In addition, the language of Set Theory contains the expression "$\{\ldots\}$," used to introduce new sets. So, for example, if $p(x)$ is a one-variable predicate, then $\{x : p(x)\}$ stands for "the set of all x for which $p(x)$ is true."

This creates some minor difficulties. For example, the introduction of the "$\{\ldots\}$" notation would mean that **we are no longer dealing with a first-order predicate calculus.** (Reason: in a first-order predicate calculus, we combine individuals[2] and function symbols to make **terms**, and then we combine terms to make **formulas**, but we never "go back" and use formulas to make terms. In Set Theory, with the "$\{\ldots\}$" notation, we can use individuals and function symbols to make terms, then terms can be used to make formulas, but then we can make bigger terms from the formulas. For example, we can use the individual letter x as a term, then this term can be used in formulas, e.g. $x = x$ and $\sim x = x$, and then from these formulas we can make the "terms" $\{x : x = x\}$ and $\{x :\sim x = x\}$.)

To avoid these problems, we will treat all expressions involving "$\{\ldots\}$" as just abbreviations of expressions in the first-order predicate calculus with $=$ and $\in$ but **without** "$\{\ldots\}$." This means that:

THE ABBREVIATION "$\{\ldots\}$"

ABBR.3: If, x is a variable, $p(x)$ is a formula not containing quantifiers in x, and t is a term not containing x, then the equality

$$t = \{x : p(x)\}$$

is an alternative way of writing

$$(\forall x)(x \in t \Leftrightarrow p(x)) .$$

Moreover, we will only introduce the "$\{\ldots\}$" notation in one way, namely, by means of equalities such as $a = \{x : p(x)\}$. This means that **every formula involving "$\{\ldots\}$"-expressions can be rewritten as a formula without the "$\{\ldots\}$s." In this way, the formulas of Set Theory "really" do not have any "$\{\ldots\}$s" at all, so they are *bona fide* formulas of a first-order predicate calculus.**

Here are the basic axioms of "Naïve" Set Theory:

[1] A **reserved constant** is a symbol—such as 1 or π or $\emptyset$—that is taken to be a constant once and for all (so the symbol can **never** be used as a variable) and has a "fixed meaning," in the sense that a definition or axiom is adopted that assigns it a meaning that will never change. Reserved constants can never be used as new constants in the application of Rule 5 and Rule 6. (For example, as explained before, if we were allowed to take the expression "$1 + 1$" and call it "1," then you would be able to prove that $1 + 1 = 1$, and this would lead to a disaster.)

[2] An "individual symbol," or "individual," for short, is a symbol, usually a letter, that is either a variable or a constant. For example, 3 is an individual symbol in arithmetic, $\emptyset$ is an individual symbol in Set Theory, the letter x is an individual symbol in the formula $(\forall x)(x.x \geq 0)$ and in the formula $x.x \geq 0$. In the former case, i.e. in $(\forall x)(x.x \geq 0)$, x is a variable. In the latter case, i.e. for $x.x \geq 0$, if such a formula ever shows up in a proof, then x will have to have been declared to be a constant earlier, e.g. by saying something like "let x be arbitrary" or "let x be such that $x > 0$," or "let $x = 5$" (which is just an alternative way of saying "let x be such that $x = 5$").

THE AXIOMS[a] OF NAÏVE SET THEORY

AXIOM-SCHEME[b] NST.1: If $p(x)$ is any formula containing the variable x, no quantifiers involving x, and no other free variable, and S is a variable that does not occur in $p(x)$, then then $(\exists S)(S = \{x : p(x)\})$ is an axiom.

AXIOM NST.2: $(\forall S)(\forall T)(S = T \Leftrightarrow (\forall x)(x \in S \Leftrightarrow x \in T))$.

AXIOM-DEFINITION NST.3: $\emptyset = \{x :\sim x = x\}$.

[a]NOTE: A completely precise statement of Axiom-scheme NST.1 needs *formulas with parameters*, as will be explained later, when we introduce *Axiomatic Set Theory*.

[b]Why do we call this an "axiom-scheme" rather than an "axiom"? Because an axiom is supposed to be a fixed formula, and NST.1 is not a fixed formula. It is a collection of formulas, one for each choice of $p(x)$. For example, NST.1 tells us that $(\exists S)(S = \{x : x = x\})$ is an axiom, that $(\exists S)(S = \{x : x \in x\})$ is an axiom, that $(\exists S)(S = \{x :\sim x \in x\})$ is an axiom, that $(\exists S)(S = \{x : \emptyset \in x\})$ is an axiom, that $(\exists S)(S = \{x : (\forall y)(\emptyset \in y \Rightarrow y \in x)\})$ is an axiom, and so on. So for each $p(x)$ NST.1 gives us an axiom. So NST.1 is a *procedure—or "scheme"–for generating axioms* rather than a single axiom.

SOME SET-THEORY DEFINITIONS

In addition to the basic symbols $\emptyset$, $\in$ and $=$, we also want to use some other symbols, such as:

- the two-argument function symbols $\cup$, $\cap$, $-$ and Δ (union, intersection, set difference and symmetric difference); these symbols are written between the two arguments, so we write $A \cup B$, $A \cap B$, $A - B$, $A \Delta B$ rather than $\cup(A, B)$, $\cap(A, B)$, $-(A, B)$, $\Delta(A, B)$; we read $A \cup B$ as "A union B," $A \cap B$ as "A intersection B," $A - B$ as "A minus B," and $A \Delta B$ as "A symmetric difference B," or "the symmetric difference of A and B;"
- the one-argument function symbols $\mathcal{P}$ and $\tilde{}$ (set of subsets of, and complement of); the "complement" symbol is written *on top* of the argument, so we write $\widetilde{A}$ rather than $\tilde{}(A)$;
- the two-argument predicate symbol $\subseteq$ (subset of), written between its two arguments, so that we write $A \subseteq B$ (and read "A is a subset of B") instead of writing $\subseteq(A, B)$.

The basic axioms only talk about $\emptyset$, $=$ and $\in$, so using these axioms alone we would have no idea of what $\cup$, $\cap$, etc. mean, and we would not be able to prove anything involving these new symbols. This means that we need, in addition, statements involving the new symbols so we can prove things about them. You can think of these statements as new axioms—giving us the basic properties of $\cup$, $\cap$, etc.—or as definitions, telling us what $\cup$, $\cap$, etc. mean.

AXIOM-DEFINITION NST.AD.1 (union): $\boxed{(\forall A)(\forall B)(A \cup B = \{x : x \in A \vee x \in B\}).}$

INFORMAL VERSION OF THE DEFINITION OF "UNION": If A, B are sets, then the **union** of A and B is the set $A \cup B$ given by $A \cup B = \{x : x \in A \vee x \in B\}$.

AXIOM-DEFINITION NST.AD.2 (intersection): $\boxed{(\forall A)(\forall B)(A \cap B = \{x : x \in A \wedge x \in B\}).}$

INFORMAL VERSION OF THE DEFINITION OF "INTERSECTION": If A, B are sets, then the **intersection** of A and B is the set $A \cap B$ given by $A \cap B = \{x : x \in A \wedge x \in B\}$.

AXIOM-DEFINITION NST.AD.3 (set inclusion):
$\boxed{(\forall A)(\forall B)(A \subseteq B \Leftrightarrow (\forall x)(x \in A \Rightarrow x \in B)).}$

INFORMAL VERSION OF THE DEFINITION OF "INCLUSION": If A, B are sets, then we say that A is a **subset** of B if, whenever x belongs to A, it follows that x belongs to B.

AXIOM-DEFINITION NST.AD.4 (the "power set"—or set of subsets—of a set):
$\boxed{(\forall A)(\mathcal{P}(A) = \{X : X \subseteq A\}).}$

INFORMAL VERSION OF THE DEFINITION OF "POWER SET": The **power set** of a set A is the set $\mathcal{P}(A)$ of all subsets of A.

AXIOM-DEFINITION NST.AD.5 (the complement of a set): $\boxed{(\forall A)(\widetilde{A} = \{x : \sim x \in A\}).}$

INFORMAL VERSION OF THE DEFINITION OF "COMPLEMENT": The **complement** of a set A is the set of all things that do not belong to A.

AXIOM-DEFINITION NST.AD.6 (set difference):
$\boxed{(\forall A)(\forall B)(A - B = \{x : x \in A \wedge (\sim x \in B)\}).}$

INFORMAL VERSION OF THE DEFINITION OF "SET DIFFERENCE": The **difference** of two sets A, B is the set $A - B$ of all things that belong to A but do not belong to B.

AXIOM-DEFINITION NST.AD.7 (symmetric difference):
$\boxed{(\forall A)(\forall B)(A \,\Delta\, B = (A - B) \cup (B - A)).}$

INFORMAL VERSION OF THE DEFINITION OF "SYMMETRIC DIFFERENCE": The **symmetric difference** of two sets A, B is the set $A \,\Delta\, B$ of all things that belong to one of the sets but do not belong to both of them.

COMMENTS:

- You will often find in books the statement that "the definition of equality of sets is that two sets S and T are **equal** if $(\forall x)(x \in S \Leftrightarrow x \in T)$." We are taking this "definition" to be an **axiom** instead but, as was explained earlier, this is not much of a distinction, because axioms and definitions function exactly the same way in proofs, so one cannot really tell a definition from an axiom.

- A more serious problem is the following: shouldn't we have said in Axiom NST.2 that $S = T \Leftrightarrow (\forall x)(x \in S \Leftrightarrow x \in T)$ *if S and T are sets*? If S and T are not sets, then presumably S and T can have the same members without being the same things. For example: I am not a set, so nothing belongs to me in the set-theory sense. If we let $\emptyset$ denote the empty set, and use S to denote me, then $(\forall x)(x \in S \Leftrightarrow x \in \emptyset)$ is true. (Proof: let x be arbitrary. Then $\sim x \in S$, because nothing belongs to me in the set-theory sense. Also, $\sim x \in \emptyset$, because nothing belongs to the empty set. So both $x \in S$ and $x \in \emptyset$ are false, and therefore the equivalence $x \in S \Leftrightarrow x \in \emptyset$ is true. Since x was arbitrary, $(\forall x)(x \in S \Leftrightarrow x \in \emptyset)$ is true.) Does this mean that I am the empty set? I would very much want to believe that the answer is "no," but in that case it seems that we have contradicted Set Axiom NST.2.

- The reason that we stated the axiom as we did is that we want to think of set theory as being *just about sets*, which means that we want to interpret it in a universe of discourse where **everything is a set**. So, when I write $(\forall S)\ldots$ in set theory, this automatically means "for all sets S ...".

- At this point, you will obviously come up with the following powerful objection: we definitely **do** want to use sets to study things other than sets, for example, numbers. We want to talk about sets of real numbers, such as, for example, intervals. So not everything is a set, even in Mathematics, because there are other things such as, for example, numbers and functions.

- This objection will be taken care of later, in two ways:

– First, we will discuss at a later point a "hybrid" set theory in which there are sets and there are also other things. In that theory, some variables will take values over sets, and some other variables will take non-set values, such as numbers. When we develop the "hybrid" theory, we will have to be careful to make sure that Set Axiom NST.2 is stated so as to apply only to sets S and T.

– The second way is harder to describe right now, but happens to be much nicer. Mathematicians have managed to construct a "mathematical universe" in which **there is nothing other than sets.** In this universe, numbers and functions are just special kinds of sets. (For example, the number 0 is the empty set, the number 1 is the one-element set whose only member is the empty set, that is, $1 = \{\emptyset\}$, the number 2 is the two-element set whose members are 0 and 1, the number 3 is the three-element set whose members are 0, 1, and 2, and so on. One can easily obtain 0 and all the natural numbers this way. To get the other integers, such as -1, -2, and so on, and all the rational numbers, as special sets, is also possible, though a bit more work is required. Finally, one can get the real numbers, functions, and everything else.) Once we reach this point, you will see that in Mathematics we can always work with **just sets and nothing but sets, because it's all sets and there is nothing else.**

EXAMPLES OF SET-THEORY PROOFS

THEOREM 1: $(\forall A)(\emptyset \subseteq A)$.

INFORMAL STATEMENT OF THEOREM 1: If A is a set, then the empty set is a subset of A.

INFORMAL PROOF: Let A be an arbitrary set. We want to prove that $\emptyset \subseteq A$, i.e. that whenever $x \in \emptyset$ it follows that $x \in A$. Let a be arbitrary. Assume $a \in \emptyset$. Since $\emptyset$ is, by definition, the set of those x such that $\sim x = x$, the fact that $a \in \emptyset$ implies $\sim a = a$. But $x = x$ for all x by Axiom Eq.1, so in particular $a = a$. So we have shown that $\sim a = a$ and $a = a$. So we have the contradiction $(\sim a = a) \wedge a = a$. From this anything follows, in particular $a \in A$. So assuming that $a \in \emptyset$ we got $a \in A$. Since a was arbitrary, this implies the desired conclusion $\emptyset \subseteq A$. **QED**

FORMAL PROOF:

(1) $(\forall X)(\forall Y)(X \subseteq Y \Leftrightarrow (\forall x)(x \in X \Rightarrow x \in Y))$. [Axiom-Definition NST.AD.3]
(2) $(\forall Y)(\emptyset \subseteq Y \Leftrightarrow (\forall x)(x \in \emptyset \Rightarrow x \in Y))$. [Rule 4, from (1)]
(3.&) Let $\bar{A}$ be arbitrary. [Preparation to apply Rule 5]
(4.&) $\emptyset \subseteq \bar{A} \Leftrightarrow (\forall x)(x \in \emptyset \Rightarrow x \in \bar{A})$. [Rule 4, from (2)]
(5.&.&) Let a be arbitrary. [Preparation to apply Rule 5]
(6.&.&.&) Assume $a \in \emptyset$. [Preparation to apply Rule 3]
(7.&.&.&) $\emptyset = \{x :\sim x = x\}$. [Axiom-definition NST.3]
(8.&.&.&) $(\forall x)(x \in \emptyset \Leftrightarrow \sim x = x)$. [Expand (7) using ABBR.3]
(9.&.&.&) $a \in \emptyset \Leftrightarrow (\sim a = a)$. [Rule 4, from (8)]
(10.&.&.&) $(a \in \emptyset \Leftrightarrow (\sim a = a)) \Rightarrow (a \in \emptyset \Rightarrow (\sim a = a))$. [Tautology $(\alpha \Leftrightarrow \beta) \Rightarrow (\alpha \Rightarrow \beta)$]
(11.&.&.&) $a \in \emptyset \Rightarrow (\sim a = a)$. [Modus Ponens from (9) and (10)]
(12.&.&.&) $\sim a = a$. [Modus Ponens from (6) and (11)]
(13.&.&.&) $(\forall x)(x = x)$. [Axiom Eq.1]
(14.&.&.&) $a = a$. [Rule 4, from (13)]
(15.&.&.&) $a = a \Rightarrow ((\sim a = a) \Rightarrow a \in \bar{A})$. [Tautology $\alpha \Rightarrow ((\sim \alpha) \Rightarrow \beta)$]
(16.&.&.&) $(\sim a = a) \Rightarrow a \in \bar{A}$. [Modus Ponens from (14) and (15)]
(17.&.&.&) $a \in \bar{A}$. [Modus Ponens from (12) and (16)]
(18.&.&) $a \in \emptyset \Rightarrow a \in \bar{A}$. [Rule 3 from (6) and (17)]
(19.&) $(\forall x)(x \in \emptyset \Rightarrow x \in \bar{A})$. [Rule 4 from (5) and (18)]

(20.&) $(\emptyset \subseteq \bar{A} \Leftrightarrow (\forall x)(x \in \emptyset \Rightarrow x \in \bar{A})) \Rightarrow ((\forall x)(x \in \emptyset \Rightarrow x \in \bar{A}) \Rightarrow \emptyset \subseteq \bar{A})$.
[Tautology $(\alpha \Leftrightarrow \beta) \Rightarrow (\beta \Rightarrow \alpha)$]
(21.&) $(\forall x)(x \in \emptyset \Rightarrow x \in \bar{A}) \Rightarrow \emptyset \subseteq \bar{A}$. [Modus Ponens from (4) and (20)]
(22.&) $\emptyset \subseteq \bar{A}$. [Modus Ponens from (19) and (21)]
(23) $(\forall A)(\emptyset \subseteq A)$. [Rule 5, from (3)and (22)]
QED

THEOREM 2: $(\forall A)(\forall B)(A \subseteq A \cup B)$.

INFORMAL STATEMENT OF THEOREM 2: If A and B are sets, then A is a subset of the union of A and B.

INFORMAL PROOF: Let A, B be arbitrary sets. We want to prove that $A \subseteq A \cup B$, i.e. that whenever $x \in A$ it follows that $x \in A \cup B$. Let a be arbitrary. Assume $a \in A$. Then $a \in A \vee a \in B$. Since $A \cup B$ is, by definition, the set of those x such that $x \in A \vee x \in B$, the fact that $a \in A \vee a \in B$ implies $a \in A \cup B$. So we have shown that $a \in A \Rightarrow a \in A \cup B$. Since a was arbitrary, this implies the desired conclusion that $(\forall x)(x \in A \Rightarrow x \in A \cup B)$. **QED**

FORMAL PROOF:
(1) $(\forall X)(\forall Y)(X \subseteq Y \Leftrightarrow (\forall x)(x \in X \Rightarrow x \in Y))$. [Axiom-Definition NST.AD.3]
(2) $(\forall X)(\forall Y)(X \cup Y = \{x : x \in X \vee x \in Y\})$. [Axiom-Definition NST.AD.1]
(3.&) Let $\bar{A}$ be arbitrary. [Preparation to apply Rule 5]
(4.&.&) Let $\bar{B}$ be arbitrary. [Preparation to apply Rule 5]
(5.&.&) $(\forall Y)(\bar{A} \cup Y = \{x : x \in \bar{A} \vee x \in Y\})$. [Rule 4, from (2)]
(6.&.&) $\bar{A} \cup \bar{B} = \{x : x \in \bar{A} \vee x \in \bar{B}\}$. [Rule 4, from (5)]
(7.&.&) $(\exists S)(S = \{x : x \in \bar{A} \vee x \in \bar{B}\})$. [Set Axiom NST.1]
(8.&.&.&) Let C be such that $C = \{x : x \in \bar{A} \vee x \in \bar{B}\}$. [From (7), prep. for Rule 6]
(9.&.&.&) $C = \bar{A} \cup \bar{B}$. [Rule 8, from (6) and (8)]
(10.&.&.&) $(\forall Y)(\bar{A} \subseteq Y \Leftrightarrow (\forall x)(x \in \bar{A} \Rightarrow x \in Y))$. [Rule 4, from (1)]
(11.&.&.&) $\bar{A} \subseteq C \Leftrightarrow (\forall x)(x \in \bar{A} \Rightarrow x \in C)$. [Rule 4, from (10)]
(12.&.&.&) $\bar{A} \subseteq \bar{A} \cup \bar{B} \Leftrightarrow (\forall x)(x \in \bar{A} \Rightarrow x \in \bar{A} \cup \bar{B})$. [Rule 8, from (9) and (11)]
(13.&.&) $\bar{A} \subseteq \bar{A} \cup \bar{B} \Leftrightarrow (\forall x)(x \in \bar{A} \Rightarrow x \in \bar{A} \cup \bar{B})$. [Rule 6, from (8) and (12)]
(14.&.&.&) Let a be arbitrary. [Preparation to apply Rule 5]
(15.&.&.&.&) Assume $a \in \bar{A}$. [Preparation to apply Rule 3]
(16.&.&.&.&) $a \in \bar{A} \Rightarrow (a \in \bar{A} \vee a \in \bar{B})$. [Tautology $\alpha \Rightarrow (\alpha \vee \beta)$]
(17.&.&.&.&) $a \in \bar{A} \vee a \in \bar{B}$. [Modus Ponens from (15) and (16)]
(18.&.&.&.&) $(\forall x)(x \in \bar{A} \cup \bar{B} \Leftrightarrow (x \in \bar{A} \vee x \in \bar{B}))$. [Expand (6) using ABBR.3]
(19.&.&.&.&) $a \in \bar{A} \cup \bar{B} \Leftrightarrow (a \in \bar{A} \vee a \in \bar{B})$. [Rule 4, from (18)]
(20.&.&.&.&) $(a \in \bar{A} \vee a \in \bar{B}) \Rightarrow ((a \in \bar{A} \cup \bar{B} \Leftrightarrow (a \in \bar{A} \vee a \in \bar{B})) \Rightarrow a \in \bar{A} \cup \bar{B})$.
[Tautology $\alpha \Rightarrow ((\beta \Leftrightarrow \alpha) \Rightarrow \beta)$]
(21.&.&.&.&) $(a \in \bar{A} \cup \bar{B} \Leftrightarrow (a \in \bar{A} \vee a \in \bar{B})) \Rightarrow a \in \bar{A} \cup \bar{B}$.
[Modus Ponens from (17) and (20)]
(22.&.&.&.&) $a \in \bar{A} \cup \bar{B}$. [ModusPonens from (19) and (21)]
(23.&.&.&) $a \in \bar{A} \Rightarrow a \in \bar{A} \cup \bar{B}$. [Rule 3, from (15) and (22)]
(24.&.&) $(\forall x)(x \in \bar{A} \Rightarrow x \in \bar{A} \cup \bar{B})$. [Rule 5, from (14) and (23)]
(25.&.&) $(\bar{A} \subseteq \bar{A} \cup \bar{B} \Leftrightarrow (\forall x)(x \in \bar{A} \Rightarrow x \in \bar{A} \cup \bar{B}))$
$\Rightarrow ((\forall x)(x \in \bar{A} \Rightarrow x \in \bar{A} \cup \bar{B}) \Rightarrow \bar{A} \subseteq \bar{A} \cup \bar{B})$. [Tautology $(\alpha \Leftrightarrow \beta) \Rightarrow (\beta \Rightarrow \alpha)$]
(26.&.&) $(\forall x)(x \in \bar{A} \Rightarrow x \in \bar{A} \cup \bar{B}) \Rightarrow \bar{A} \subseteq \bar{A} \cup \bar{B}$. [Modus Ponens from (13) and (25)]
(27.&.&) $\bar{A} \subseteq \bar{A} \cup \bar{B}$. [Modus Ponens from (24) and (26)]
(28.&) $(\forall B)(\bar{A} \subseteq \bar{A} \cup B)$. [Rule 5, from (4) and (27)]
(29) $(\forall A)(\forall B)(A \subseteq A \cup B)$. [Rule 5, from (3) and (28)]
QED

THEOREM 3: $(\forall A)(\forall B)(A \subseteq B \Leftrightarrow A = A \cap B)$.

INFORMAL STATEMENT OF THEOREM 3: If A and B are sets, then $A \subseteq B$ if and only if $A = A \cap B$.

INFORMAL PROOF: Let A, B be arbitrary sets. Assume that $A \subseteq B$. We want to prove that $A = A \cap B$. Let $a \in A$. Then $a \in B$ as well, because $A \subseteq B$. So $a \in A \cap B$. Conversely, assume $a \in A \cap B$. Then $a \in A$ and $a \in B$. In particular, $a \in A$. So we have shown that $a \in A$ implies $a \in A \cap B$ and $a \in A \cap B$ implies $a \in A$. Therefore $a \in A \Leftrightarrow a \in A \cap B$. Since a was arbitrary, $A = A \cap B$.

We now prove the converse, that is, we assume that $A = A \cap B$ and prove that $A \subseteq B$. Let $a \in A$. Then $a \in A \cap B$, because $A = A \cap B$. So $a \in A$ and $a \in B$. In particular, $a \in B$. So we have shown that $a \in A \Rightarrow a \in B$. Sicne a was arbitrary, $a \subseteq B$, as desired. **QED**

FORMAL PROOF:

(1)	$(\forall X)(\forall Y)(X \cap Y = \{x : x \in X \wedge x \in Y\})$.	[Axiom-definition NST.AD.2]
(2)	$(\forall X)(\forall Y)(X \subseteq Y \Leftrightarrow (\forall x)(x \in X \Rightarrow x \in Y))$.	[Axiom-definition NST.AD.3]
(3)	$(\forall S)(\forall T)(S = T \Leftrightarrow (\forall x)(x \in S \Leftrightarrow x \in T))$.	[Set Axiom NST.2]
(4.&)	Let $\bar{A}$ be arbitrary.	[Preparation to apply Rule 5]
(5.&.&)	Let $\bar{B}$ be arbitrary.	[Preparation to apply Rule 5]
(6.&.&)	$(\forall Y)(\bar{A} \subseteq Y \Leftrightarrow (\forall x)(x \in \bar{A} \Rightarrow x \in Y))$.	[Rule 4, from (2)]
(7.&.&)	$\bar{A} \subseteq \bar{B} \Leftrightarrow (\forall x)(x \in \bar{A} \Rightarrow x \in \bar{B})$.	[Rule 4, from (6)]
(8.&.&)	$(\forall Y)(\bar{A} \cap Y = \{x : x \in \bar{A} \wedge x \in Y\})$.	[Rule 4, from (1)]
(9.&.&)	$\bar{A} \cap \bar{B} = \{x : x \in \bar{A} \wedge x \in \bar{B}\}$.	[Rule 4, from (8)]
(10.&.&)	$(\exists S)(S = \{x : x \in \bar{A} \wedge x \in \bar{B}\})$.	[Set Axiom NST.1]
(11.&.&.&)	Let C be such that $C = \{x : x \in \bar{A} \wedge x \in \bar{B}\}$.	[From (10), prep. for Rule 6]
(12.&.&.&)	$C = \bar{A} \cap \bar{B}$.	[Rule 8, from (9) and (11)]
(13.&.&.&)	$(\forall T)(\bar{A} = T \Leftrightarrow (\forall x)(x \in \bar{A} \Leftrightarrow x \in T))$.	[Rule 4, from (3)]
(14.&.&.&)	$\bar{A} = C \Leftrightarrow (\forall x)(x \in \bar{A} \Leftrightarrow x \in C)$.	[Rule 4, from (13)]
(15.&.&.&)	$\bar{A} = \bar{A} \cap \bar{B} \Leftrightarrow (\forall x)(x \in \bar{A} \Leftrightarrow x \in \bar{A} \cap \bar{B})$.	[Rule 8, from (12) and (14)]
(16.&.&.&)	$(\forall x)(x \in \bar{A} \cap \bar{B} \Leftrightarrow (x \in \bar{A} \wedge x \in \bar{B}))$.	[Expand (9) using ABBR.3]
(17.&.&.&.&)	Assume $(\forall x)(x \in \bar{A} \Leftrightarrow x \in \bar{A} \cap \bar{B})$.	[Preparation to apply Rule 3]
(18.&.&.&.&.&)	Let a be arbitrary.	[Preparation to apply Rule 5]
(19.&.&.&.&.&)	$a \in \bar{A} \Leftrightarrow a \in \bar{A} \cap \bar{B}$.	[Rule 4, from (17)]
(20.&.&.&.&.&)	$a \in \bar{A} \cap \bar{B} \Leftrightarrow (a \in \bar{A} \wedge a \in \bar{B})$.	[Rule 4, from (16)]
(21.&.&.&.&.&)	$(a \in \bar{A} \Leftrightarrow a \in \bar{A} \cap \bar{B})$ $\Rightarrow ((a \in \bar{A} \cap \bar{B} \Leftrightarrow (a \in \bar{A} \wedge a \in \bar{B})) \Rightarrow (a \in \bar{A} \Rightarrow a \in \bar{B}))$.	[Tautology $(\alpha \Leftrightarrow \beta) \Rightarrow ((\beta \Leftrightarrow (\gamma \wedge \delta) \Rightarrow (\alpha \Rightarrow \delta))$]
(22.&.&.&.&.&)	$(a \in \bar{A} \cap \bar{B} \Leftrightarrow (a \in \bar{A} \wedge a \in \bar{B})) \Rightarrow (a \in \bar{A} \Rightarrow a \in \bar{B})$.	[Modus Ponens from (19) and (21)]
(23.&.&.&.&.&)	$a \in \bar{A} \Rightarrow a \in \bar{B}$.	[Modus Ponens from (20) and (22)]
(24.&.&.&.&)	$(\forall x)(x \in \bar{A} \Rightarrow x \in \bar{B})$.	[Rule 5, from (18) and (23)]
(25.&.&.&)	$(\forall x)(x \in \bar{A} \Leftrightarrow x \in \bar{A} \cap \bar{B}) \Rightarrow (\forall x)(x \in \bar{A} \Rightarrow x \in \bar{B})$.	[Rule 3, from (17) and (24)]
(26.&.&.&.&)	Assume $(\forall x)(x \in \bar{A} \Rightarrow x \in \bar{B})$.	[Preparation to apply Rule 3]
(27.&.&.&.&.&)	Let a be arbitrary.	[Preparation to apply Rule 5]
(28.&.&.&.&.&)	$a \in \bar{A} \Rightarrow a \in \bar{B}$.	[Rule 4, from (26)]
(29.&.&.&.&.&)	$(a \in \bar{A} \Rightarrow a \in \bar{B}) \Rightarrow (a \in \bar{A} \Leftrightarrow (a \in \bar{A} \wedge a \in \bar{B}))$.	[Tautology $(\alpha \Rightarrow \beta) \Rightarrow (\alpha \Leftrightarrow (\alpha \wedge \beta))$]
(30.&.&.&.&.&)	$a \in \bar{A} \Leftrightarrow (a \in \bar{A} \wedge a \in \bar{B})$.	[Modus Ponens from (28) and (29)]
(31.&.&.&.&.&)	$a \in \bar{A} \cap \bar{B} \Leftrightarrow (a \in \bar{A} \wedge a \in \bar{B})$.	[Rule 4, from (16)]
(32.&.&.&.&.&)	$(a \in \bar{A} \cap \bar{B} \Leftrightarrow (a \in \bar{A} \wedge a \in \bar{B}))$ $\Rightarrow ((a \in \bar{A} \Leftrightarrow (a \in \bar{A} \wedge a \in \bar{B})) \Rightarrow (a \in \bar{A} \Leftrightarrow a \in \bar{A} \cap \bar{B}))$.	[Tautology $(\alpha \Leftrightarrow \beta) \Rightarrow ((\gamma \Leftrightarrow \beta) \Rightarrow (\gamma \Leftrightarrow \alpha))$]
(33.&.&.&.&.&)	$(a \in \bar{A} \Leftrightarrow (a \in \bar{A} \wedge a \in \bar{B})) \Rightarrow (a \in \bar{A} \Leftrightarrow a \in \bar{A} \cap \bar{B})$.	[Modus Ponens from (31) and (32)]
(34.&.&.&.&.&)	$a \in \bar{A} \Leftrightarrow a \in \bar{A} \cap \bar{B}$.	[Modus Ponens from (30) and (33)]
(35.&.&.&.&)	$(\forall x)(x \in \bar{A} \Leftrightarrow x \in \bar{A} \cap \bar{B})$.	[Rule 5, from (27) and (34)]
(36.&.&.&)	$(\forall x)(x \in \bar{A} \Rightarrow x \in \bar{B}) \Rightarrow (\forall x)(x \in \bar{A} \Leftrightarrow x \in \bar{A} \cap \bar{B})$.	[Rule 3, from (26) and (35)]

Now use P as an abbreviation for $(\forall x)(x \in \bar{A} \Rightarrow x \in \bar{B})$ and use Q as an abbreviation for $(\forall x)(x \in \bar{A} \Leftrightarrow x \in \bar{A} \cap \bar{B})$.

(37.&.&.&)	$(P \Rightarrow Q) \Rightarrow ((Q \Rightarrow P) \Rightarrow (P \Leftrightarrow Q))$.	[Tautology]
(38.&.&.&)	$(Q \Rightarrow P) \Rightarrow (P \Leftrightarrow Q)$.	[Modus Ponens from (36) and (37)]
(39.&.&.&)	$P \Leftrightarrow Q$.	[Modus Ponens from (25) and (38)]
(40.&.&.&)	$(\bar{A} \subseteq \bar{B} \Leftrightarrow P) \Rightarrow ((P \Leftrightarrow Q) \Rightarrow (\bar{A} \subseteq \bar{B} \Leftrightarrow Q))$.	[Tautology $(\alpha \Leftrightarrow \beta) \Rightarrow ((\beta \Leftrightarrow \gamma) \Rightarrow (\alpha \Leftrightarrow \gamma))$]
(41.&.&.&)	$(P \Leftrightarrow Q) \Rightarrow (\bar{A} \subseteq \bar{B} \Leftrightarrow Q)$.	[Modus Ponens from (7) and (40)]
(42.&.&.&)	$\bar{A} \subseteq \bar{B} \Leftrightarrow Q$.	[Modus Ponens from (39) and (41)]
(43.&.&.&)	$(\bar{A} \subseteq \bar{B} \Leftrightarrow Q) \Rightarrow ((\bar{A} = \bar{A} \cap \bar{B} \Leftrightarrow Q) \Rightarrow (\bar{A} \subseteq \bar{B} \Leftrightarrow \bar{A} = \bar{A} \cap \bar{B}))$.	[Tautology $(\alpha \Leftrightarrow \beta) \Rightarrow ((\gamma \Leftrightarrow \beta) \Rightarrow (\alpha \Leftrightarrow \gamma))$]
(44.&.&.&)	$(\bar{A} = \bar{A} \cap \bar{B} \Leftrightarrow Q) \Rightarrow (\bar{A} \subseteq \bar{B} \Leftrightarrow \bar{A} = \bar{A} \cap \bar{B})$.	[Modus Ponens from (42) and (43)]
(45.&.&.&)	$\bar{A} \subseteq \bar{B} \Leftrightarrow \bar{A} = \bar{A} \cap \bar{B}$.	[Modus Ponens from (15) and (44)]
(46.&.&)	$\bar{A} \subseteq \bar{B} \Leftrightarrow \bar{A} = \bar{A} \cap \bar{B}$.	[Rule 6, from (11) and (45)]
(47.&)	$(\forall B)(\bar{A} \subseteq B \Leftrightarrow \bar{A} = \bar{A} \cap B)$.	[Rule 5, from (5) and (46)]
(48)	$(\forall A)(\forall B)(A \subseteq B \Leftrightarrow A = A \cap B)$.	[Rule 5, from (4) and (47)]

QED

A CATASTROPHE

THEOREM 4: $\emptyset = \emptyset \wedge (\sim \emptyset = \emptyset)$

INFORMAL STATEMENT OF THEOREM 4: The empty set is both equal to itself and not equal to itself.

INFORMAL PROOF: Let C be the set of all x such that x does not belong to C, that is

$$C = \{x :\sim x \in x\}\,.$$

Then, if x is arbitrary, we have $x \in C \Leftrightarrow (\sim x \in x)$. Specialize this to $x = C$. We get $C \in C \Leftrightarrow (\sim C \in C)$. Now $C \in C \Leftrightarrow (\sim C \in C)$ is an instance of the contradiction $\alpha \Leftrightarrow (\sim \alpha)$. So, if P is any statement whatsoever, then $(C \in C \Leftrightarrow (\sim C \in C)) \Rightarrow P$ is an instance of the tautology $(\alpha \Leftrightarrow (\sim \alpha)) \Rightarrow \beta$. Now we can take P to be any statement we want, for example $\emptyset = \emptyset \wedge (\sim \emptyset = \emptyset)$. Then $(C \in C \Leftrightarrow (\sim C \in C)) \Rightarrow P$ is an instance of a tautology, and we have proved $C \in C \Leftrightarrow (\sim C \in C)$. So we get P by Modus Ponens. **QED**

FORMAL PROOF:

(1)	$(\exists S)(S = \{x :\sim x \in x\})$.	[Set Axiom NST.1]
(2.&)	Let C be such that $C = \{x :\sim x \in x\})$.	[From (1), in preparation to apply Rule 6]
(3.&)	$(\forall x)(x \in C \Leftrightarrow (\sim x \in x))$.	[Expand (2) using ABBR.3]
(4.&)	$C \in C \Leftrightarrow (\sim C \in C)$.	[Rule 4, from (3)]
(5.&)	$(C \in C \Leftrightarrow (\sim C \in C)) \Rightarrow (\emptyset = \emptyset \wedge (\sim \emptyset = \emptyset))$.	[Tautology $(\alpha \Leftrightarrow (\sim \alpha)) \Rightarrow \beta$]
(6.&)	$\emptyset = \emptyset \wedge (\sim \emptyset = \emptyset)$.	[Modus Ponens from (4) and (5)]
(7)	$\emptyset = \emptyset \wedge (\sim \emptyset = \emptyset)$.	[Rule 6, from (2) and (6)]

QED

THE RUSSELL PARADOX

Theorem 4 has catastrophic consequences, because **its conclusion is a contradiction.** So Theorem 4 tells us that

$$\boxed{\mathcal{NA\ddot{I}VE\ SET\ THEORY\ IS\ INCONSISTENT}!!!}$$

This means that **in Naïve Set Theory you can prove anything you want.** For example, you can prove that $2 + 2 = 4$, that $2 + 2 = 7$, that the number 5 is prime, that the number 5 isn't prime, that $\sqrt{2}$ is irrational, that $\sqrt{2}$ is rational, that you are the Emperor of the Klingorns, anything you want. (We saw in one of the boxes in Handout No. 10—in page 3—how, once you have prved one contradiction, it becomes possible to prove absolutely anything.) This means that the whole idea of developing a mathematical theory based on Naïve Set Theory is just pointless, because the notion of proof becomes useles, since every statement is provable, so we can prove false things as well as true ones, and if we prove something then we will still don't know that it is true.
The inconsistency of Naïve Set Theory was discovered by the British mathematician and philosopher **Bertand Russell** (1872-1970[1]):

> Over a long and varied career, Bertrand Russell made ground-breaking contributions to the foundations of mathematics and to the development of contemporary formal logic, as well as to analytic philosophy. His contributions relating to mathematics include his discovery of Russell's paradox, his defense of logicism (the view that mathematics is, in some significant sense, reducible to formal logic), his introduction of the theory of types, and his refining and popularizing of the first-order predicate calculus. Along with Kurt Gödel, he is usually credited with being one of the two most important logicians of the twentieth century.
> Russell discovered the paradox which bears his name in May 1901, while working on his Principles of Mathematics (1903). The paradox arose in connection with the set of all sets which are not members of themselves. Such a set, if it exists, will be a member of itself if and only if it is not a member of itself. The significance of the paradox follows since, in classical logic, all sentences are entailed by a contradiction. In the eyes of many mathematicians (including David Hilbert and Luitzen Brouwer) it therefore appeared that **no proof could be trusted once it was discovered that the logic apparently underlying all of mathematics was contradictory.** A large amount of work throughout the early part of this century in logic, set theory, and the philosophy and foundations of mathematics was thus prompted.
> Russell's paradox arises as a result of naïve set theory's so-called unrestricted comprehension (or abstraction) axiom. Originally introduced by Georg Cantor, the axiom states that any predicate expression, $P(x)$, which contains x as a free variable, will determine a set whose members are exactly those objects which satisfy $P(x)$. The axiom gives form to the intuition that any coherent condition may be used to determine a set (or class). Most attempts at resolving Russell's paradox have therefore concentrated on various ways of restricting or abandoning this axiom.

NOTE: The above quotation is taken from the Web page

http://www-groups.dcs.st-and.ac.uk/~history/ShortBiogs.html

This Web site contains a lot of biographical information about mathematicians. I strongly recommend that you pay it a visit.

[1] Yes, he lived 97 years! He was born on May 18, 1872, and died on Feb 2, 1970.

FREGE

Gottlob Frege (1848-1925) was one of the founders of modern symbolic logic putting forward the view that mathematics is reducible to logic.

Frege received his education at the universities of Jena (1869-71) and Göttingen (1871-1873) where he studied mathematics, physics and chemistry. He then taught at Jena in the department of mathematics where he remained, first as a lecturer and then as a professor, for the rest of his working life.

Frege lectured on all branches of mathematics although his mathematical publications outside the field of logic are few. His writings on the philosophy of logic, philosophy of mathematics, and philosophy of language are of major importance. He once said: "Every good mathematician is at least half a philosopher, and every good philosopher is at least half a mathematician."

He was the first to fully develop the main thesis of logicism, that mathematics is reducible to logic. His works *The Foundations of Arithmetic* (1884) and *The Basic Laws of Arithmetic, Volume 1* (1893) are devoted to this project.

His work was not particularly well received, mainly it was ignored. While Volume 2 of *The Basic Laws of Arithmetic* was at the printers he received a letter (on June 16, 1902) from Bertrand Russell. Russell pointed out, with great modesty, that the Russell paradox gave a contradiction in Frege's system of axioms. After many letters between the two Frege modified one of his axioms and explains in an appendix to the book that this was done to restore the consistency of the system. However with this modified axiom, many of the theorems of Volume 1 do not go through and Frege must have known this. He probably never realized that even with the modified axiom the system is inconsistent since this was not shown until after Frege's death by Leshniewski.

NOTE: This material is taken from the Web page
http://www-groups.dcs.st-and.ac.uk/~history/ShortBiogs.html

RUSSEL'S ARGUMENT

The argument used by Russell to get his paradox is as follows:

> Form the set
> $$S = \{x : x \notin x\}.$$
> Does S belong to S or not? If $S \in S$ then S must be one of the x's that satisfy the condition defining S, namely, $x \notin x$. So $S \notin S$. If $S \notin S$ then S is one of the x's that satisfy the condition defining S, namely, $x \notin x$, so $S \in S$. So we have proved $S \in S \iff S \notin S$, which is a contradiction.

This belongs to a long tradition of "paradoxes," going back to classical Greece. For example:

- Suppose I say "What I am saying now is a lie." Is this true of false? You can see right away that if it is true then it has to be false, and if it is false then it has to be true.
- Suppose there is a town where some men shave themselves and other do not. Suppose the town's barber shaves those people who do not shave themselves, and nobody else. Does he shave himself?

The common denominator of all these paradoxes is **self-reference**. "What I am saying now is a lie" is a *self-referential statement*, because it talks about itself. (The statement says, essentially, "I am not true.") Similarly, if S is the set of Russell's paradox, then the statement $S \in S$ can only be true if it is not true, so the statement says "I am not true."

WHY IS A SINGLE CONTRADICTION SO BAD?

People who learn for the first time about the Russell paradox often fail to appreciate how devastating it is. Sure, one can prove a contradiction about some very weird set, but so what? Nobody cares about weird sets anyhow, so this should not pose any problem when we want to prove theorems about "really important" mathematical objects such as natural numbers and real numbers.
We already showed that this argument doesn't suffice. Indeed, once a contradiction can be proved *somewhere*, then the whole edifice of logic collapses, because **everything** can be proved, so proofs become worthless.
It is said that Bertrand Russell was giving a lecture once on this topic, and at the end someone asked, incredulously:

> I don't see how one can prove anything whatsoever from just one contradiction. For example, let us suppose that I allow you to assume that $1 = 0$. Can you prove that you are the Pope?

Russel's response came quickly:

> Sure I can. Here is the proof. If $1 = 0$ then, adding 1 to both sides, we get $2 = 1$. Now, let A be the set consisting of two people, namely, myself and the Pope. Then A has two members. Since $2 = 1$, A has exactly one member. Therefore the Pope and I are the same person. So I am the Pope. **QED**

AXIOMATIC SET THEORY

Axiomatic Set Theory arises as an effort to eradicate the Russell paradox from Set Theory. If you look at the proof of Theorem 4, you will see that the real culprit appears to be Set Axiom NST.1, which allowed us to bring in the set $\{x :\sim x \in x\}$. This axiom is called the "comprehension" or "abstraction" axiom, because it allows us to "abstract"[3] a property—represented by a predicate $p(x)$— and form the set of all the things that have this property. Axiom NST.2 is an **unrestricted abstraction axiom**, because it allows to manufacture a set for every property. If this is allowed, then we can take the predicate $\sim x \in x$, and the result is unmitigated disaster, as we have shown.

The way to get around this problem is to restrict the validity of the abstraction axiom.

THE BASIC AXIOMS OF AXIOMATIC SET THEORY

In Axiomatic Set Theory, we use the same basic symbols as in Naïve Set Theory, namely, the binary predicate symbols $=$ and $\in$, and the reserved constant $\emptyset$. The three basic axioms are:

AXIOM-SCHEME AST.1: If $S, T, x, y_1, \ldots, y_n$ are distinct variables, and $p(x, y_1, \ldots, y_n))$ is any formula that has no quantifiers involving $x, y_1, \ldots, y_n$, has no free variables other than $x, y_1, \ldots, y_n$, does not contain S, and does not contain T, then

$$(\forall y_1) \ldots (\forall y_n)(\forall T)(\exists S)(S = \{x : x \in T \wedge p(x, y_1, y_2, \ldots, y_n)\})$$

is an axiom.

AXIOM AST.2: $(\forall S)(\forall T)(S = T \Leftrightarrow (\forall x)(x \in S \Leftrightarrow x \in T))$.

AXIOM-DEFINITION AST.3: $\emptyset = \{x :\sim x = x\}$.

[3] The verb "to abstract" means "to take out of; extract; remove; consider separately from something else."

COMMENTS:

- The second and third axioms (that is, the "definitions" of equality and the empty set) are exactly the same as in Naïve Set Theory.
- The first axiom is quite different, however. To understand the difference, let us first forget about the variables $y_1, \ldots, y_n$ and just focus on the main difference. In Naïve Set Theory we said that if $p(x)$ is a formula that does not contains the variable S, has no free variables other than x, and contains no quantifiers in x, then

  $$(\exists S)(S = \{x : p(x)\})$$

  is an axiom. Now we are saying that

  $$(\forall T)(\exists S)(S = \{x : x \in T \wedge p(x)\}) \qquad (\%)$$

  is an axiom, if in addition $p(x)$ does not contain T either.

  So, for example, in Naïve Set Theory we can take $p(x)$ to be the formula $\sim x \in x$, and conclude that

  $$(\exists S)(S = \{x :\sim x \in x\}) \qquad (*)$$

  is an axiom. Then we can bring (*) into a proof, as we did in Step 1 of the proof of Theorem 4, with disastrous consequences.

  In Axiomatic Set Theory, all we can conclude is that

  $$(\forall T)(\exists S)(S = \{x : x \in T \wedge (\sim x \in x)\}) \qquad (\#)$$

  is an axiom. Then you can bring (#) into a proof, but you will not be able to do anything with it unless you get hold of some set A, so that you can specialize T to A is (#) and go to

  $$(\exists S)(S = \{x : x \in A \wedge (\sim x \in x)\}) .$$

  This will give you new set whose members are all the xs such that $x \in A$ and $\sim x \in x$. Clearly, this set will be a subset of A. The Russell paradox does not arise any more.

  Actually, Axiom-scheme AST.1 will only allow you to build new sets as subsets of old sets. If $p(x)$ is a formula as before, then (%) is an axiom, but you will only be able to use this to produce the set $\{x : x \in A \wedge p(x)\}$ out of a set A already known to exist, and what you will get will be a subset of A.

  So Axiom-scheme AST.1 is a **restricted abstraction axiom**, because it allows us to form new sets by "abstraction," but it only does so under very restricted conditions.

SOME OTHER AXIOMS OF AXIOMATIC SET THEORY

By introducing the restricted abstraction axiom of Axiomatic Set Theory as a substitute for the unrestricted abstraction axiom of Naïve Set Theory, we avoid the Russell paradox. But we have to pay a price. If we can only form new sets by "extracting" them from old sets, it would seem that we can never a large set if we only have small sets.

For example: suppose we have a set A. How do we know that the power set $\mathcal{P}(A)$ exists? Similarly, suppose we have two sets A and B. How do we know that the union $A \cup B$ exists?

In *some* cases, we can prove existence. For example, let us prove that the intersection of two sets always exists. ("Intersection" is defined by Axiom-definition (NST.AD.2), exactly as in Naïve Set Theory.)

THEOREM 5: $(\forall A)(\forall B)(\exists C)(C = A \cap B)$.

INFORMAL PROOF: Let A, B be sets. Then the restricted abstraction Axiom-scheme AST.1 tells us that there is a set C such that $C = \{x : x \in A \wedge (x \in A \wedge x \in B)\}$. Since "$x \in A \wedge (x \in A \wedge x \in B)$" is obviously equivalent to "$x \in A \wedge x \in B$," C is none other than $\{x : x \in A \wedge x \in B\}$. So $C = A \cap B$. **QED**

FORMAL PROOF:

(1) $(\forall X)(\forall Y)(X \cap Y = \{x : x \in X \wedge x \in Y\})$. [Axiom-definition NST.AD.2]

(2) $(\forall X)(\forall Y)(\forall T)(\exists S)(S = \{x : x \in T \wedge (x \in X \wedge x \in Y)\})$. [Axiom-scheme AST.1]

NOTE: We are applying AST.1 with $n = 2$, using the formula $x \in X \wedge x \in Y$—which has three variables, namely, x, X, and Y—in the role of p.

(3.&) Let $\bar{A}$ be arbitrary. [Preparation to apply Rule 5]

(4.&.&) Let $\bar{B}$ be arbitrary. [Preparation to apply Rule 5]

(5.&.&) $(\forall Y)(\bar{A} \cap Y = \{x : x \in \bar{A} \wedge x \in Y\})$. [Rule 4, from (1)]

(6.&.&) $(\forall Y)(\forall T)(\exists S)(S = \{x : x \in T \wedge (x \in \bar{A} \wedge x \in Y)\})$. [Rule 4, from (2)]

(7.&.&) $\bar{A} \cap \bar{B} = \{x : x \in \bar{A} \wedge x \in \bar{B}\}$. [Rule 4, from (5)]

(8.&.&) $(\forall T)(\exists S)(S = \{x : x \in T \wedge (x \in \bar{A} \wedge x \in \bar{B})\})$. [Rule 4, from (6)]

(9.&.&) $(\exists S)(S = \{x : x \in \bar{A} \wedge (x \in \bar{A} \wedge x \in \bar{B})\})$. [Rule 4, from (8)]

(10.&.&.&) Let $\bar{C}$ be such that $\bar{C} = \{x : x \in \bar{A} \wedge (x \in \bar{A} \wedge x \in \bar{B})\}$. [From (9), preparation to apply Rule 6]

(11.&.&.&) $(\forall x)(x \in \bar{C} \Leftrightarrow (x \in \bar{A} \wedge (x \in \bar{A} \wedge x \in \bar{B})))$. [Expand (10) using ABBR.3]

(12.&.&.&) $(\forall x)(x \in \bar{A} \cap \bar{B} \Leftrightarrow (x \in \bar{A} \wedge x \in \bar{B}))$. [Expand (7) using ABBR.3]

(13.&.&.&.&) Let a be arbitrary. [Preparation to apply Rule 5]

(14.&.&.&.&) $a \in \bar{C} \Leftrightarrow (a \in \bar{A} \wedge (a \in \bar{A} \wedge a \in \bar{B}))$. [Rule 4, from (11)]

(15.&.&.&.&) $(a \in \bar{C} \Leftrightarrow (a \in \bar{A} \wedge (a \in \bar{A} \wedge a \in \bar{B}))) \Rightarrow (a \in C \Leftrightarrow (a \in \bar{A} \wedge a \in \bar{B}))$. [Tautology $(\alpha \Leftrightarrow (\beta \wedge (\beta \wedge \gamma))) \Rightarrow (\alpha \Leftrightarrow (\beta \wedge \gamma))$]

(16.&.&.&.&) $a \in \bar{C} \Leftrightarrow (a \in \bar{A} \wedge a \in \bar{B})$. [Modus Ponens from (14) and (15)]

(17.&.&.&) $(\forall x)(x \in \bar{C} \Leftrightarrow (x \in \bar{A} \wedge x \in \bar{B}))$. [Rule (5) from (13) and (16)]

(18.&.&.&) $\bar{C} = \{x : x \in \bar{A} \wedge x \in \bar{B}\}$. [Abbreviate (17) using ABBR.3]

(19.&.&.&) $\bar{C} = \bar{A} \cap \bar{B}$. [Rule 8, from (7) and (18)]

(20.&.&.&) $(\exists C)(C = \bar{A} \cap \bar{B})$. [Rule 7, from (19)]

(21.&.&) $(\exists C)(C = \bar{A} \cap \bar{B})$. [Rule 6, from (10) and (20)]

(22.&) $(\forall B)(\exists C)(C = \bar{A} \cap B)$. [Rule 5, from (4) and (21)]

(23) $(\forall A)(\forall B)(\exists C)(C = A \cap B)$. [Rule 5, from (3) and (22)]

QED

QUESTION: do you think you can prove in the same way that the union $A \cup B$ of any two sets A, B, exists? How about the difference $A - B$ and the symmetric difference $A \Delta B$?

HOW DO WE KNOW THAT THERE ARE ANY SETS AT ALL?

If you think about it for a minute, we could even ask

HOW DO WE KNOW THAT THERE ARE ANY SETS AT ALL ?

Or, if you remember that we are thinking of set theory as describing a world where there is nothing but sets, the question becomes

HOW DO WE KNOW IN AXIOMATIC SET THEORY THAT THERE IS ANYTHING AT ALL?

If you try to translate this into a formal statement, the question becomes

> How do we know that $(\exists x)(x = x)$ is true?

If you are baffled by the fact that we are translating "something exists" as "$(\exists x)(x = x)$," try to figure out how else you might say that "something exists." You cannot say "$(\exists x)$," because this is not a well-formed formula[4]. All you can say is that "there exists some x such that $p(x)$," if $p(x)$ is a formula. Fortunately, we can use the formula $x = x$, which is true for every x, so saying that "something exists" is exactly equivalent to saying "there exists some x such that $x = x$."

The answer to our existence question is easy, because our axioms are such that the existence of at least one set, namely, the empty set, is guaranteed.

THEOREM 6: $(\exists x)(x = x)$.

INFORMAL STATEMENT OF THEOREM 6: Something exists.

INFORMAL PROOF: By Axiom AST.3, the empty set exists. **QED**

FORMAL PROOF:

(1)	$(\forall x)(x = x)$.	[Axiom Eq.1]
(2)	$\emptyset = \emptyset$.	[Rule 4, from (1)]
(3)	$(\exists x)(x = x)$.	[Rule 7, from (2)]

QED

So we have made some progress, but not much, really. We got **one** set, namely, the empty set. Can we do better?

HOW DO WE KNOW IN AXIOMATIC SET THEORY THAT THERE ARE ANY SETS OTHER THAN THE EMPTY SET?

The answer to this and other fascinating questions is coming in the next handout.

[4] There is a serious philosophical issue underlying all this. In English, the verb "exist" functions very much like other intransitive verbs such as "sleep" or "work." You can talk about things (or people) that sleep and things that do not. In either case, the thing—or person—must exist, for otherwise who would you be talking about when you say that so-and-so sleeps eight hours a day? This sometimes has led people to think that anything you could talk about —e.g. unicorns, six-legged chickens, flying pigs, and round squares— must exist. For example, even when we say that "round squares do not exist," this looks like a statement that talks about some things—round squares—and says that those things have a certain property, namely, that of not existing. Since that statement talks about something, there must be something that the statement talks about, or else it would be talking about nothing, which looks ridiculous, since the statement clearly talks about round squares. In the formal language called "predicate calculus," this problem disappears, because "exists" is not a predicate at all. "Exists" is a **quantifier**, which means that we can say things like "$\sim (\exists x)(x$ is square $\wedge\, x$ is round$)$," but this does not in any way mean that we are talking about an existing object. All it means is that there is no way to fill the square slot in the expression "$\square$ is square $\wedge$ $\square$ is round" so as to make the resulting statement true.