國立臺灣大學課程綱要格式

課程資訊					
課程名稱	軟體規格與驗證				
課程編號	725 U3220	班次		學分數	3
全/半年	半年			必/選修	選修
授課教師	蔡益坤			開課系所	資訊管理學研究所
上課時間	星期三 上午 9:10--12:10			上課地點	管院二館 302
備註	當修課人數較少時，我們在管院二館 11 樓研討室上課。 授課教師研究室：管院二館 1108；電話：3366-1189				
課程網頁	http://im.ntu.edu.tw/~tsay/courses/ssv/				
課程大綱					
為確保您我的權利,請尊重智慧財產權及不得非法影印					
課程目標	使學生熟悉正規軟體驗證的基礎知識，為未來在該領域從事研究做好準備。				
課程概述	本課程為正規軟體規格與驗證之入門課程,涵蓋用於描述軟體程式性質及證明特定軟體確實滿足其性質的正規語言、方法及工具。我們將專注在演譯式的方法〔包括定理證明〕。另一門與本課程互補，名為「自動化軟體驗證」的課程則專注在演算式的方法〔包括模型檢驗〕。我們將兼顧廣度與廣度深度，不僅研習基礎的原理，也探究一些較成功的正規語言、技術及工具。				
關鍵字	正規方法、邏輯、程式正確性、軟體驗證、定理證明				
課程要求	本課程包括期末考、數次作業、及一篇期末報告。 每位同學同時必須就一個選定的主題在課堂上做口頭報告,視為期末報告之一部分。				
Office Hours	星期三下午 1:30--2:30 或另行約定				
指定閱讀	Class Notes and Selected Readings (available on the course Web site)				
參考書目	1. *Logic for Computer Science*, J.H. Gallier, Harper & Row Publishers, 1985. 2. *Proof Theory and Automated Deduction*, J. Goubault-Larrecq and I. Mackie, Kluwer Academic Publishers, 1997. 3. *A Logical Approach to Discrete Math*, D. Gries and F.B. Schneider, Springer-Verlag, 1993. 4. *Foundations for Programming Languages*, J.C. Mitchell, The MIT Press, 1996.				

<table>
<tr><td></td><td>
5. Formal Syntax and Semantics of Programming Languages, K. Slonneger and B.L. Kurtz, Addison-Wesley, 1995.
6. Verification of Sequential and Concurrent Programs, 2nd Edition, K.R. Apt and E.-R. Olderog, Springer-Verlag, 1997.
7. The Science of Programming, D. Gries, Springer-Verlag, 1981.
8. Predicate Calculus and Program Semantics, E.W. Dijkstra and C.S. Scholten, Springer-Verlag, 1990.
9. Programming from Specifications, 2nd Edition, C. Morgan, 1994.
10. The Z Notation: A Reference Manual, 2nd Edition, J.M. Spivey, 1992.
11. Software Engineering with B, J.B. Wordsworth, Addison-Wesley, 1996.
12. Software Abstractions: Logic, Language, and Analysis, D. Jackson, MIT Press, 2006.
13. The Temporal Logic of Reactive and Concurrent Systems: Specification, Z. Manna and A. Pnueli, Springer-Verlag, 1992.
14. Temporal Verification of Reactive Systems: Safety, Z. Manna and A. Pnueli, Springer, 1995.
15. Temporal Verification of Reactive Systems: Progress, Z. Manna and A. Pnueli, Book Draft, 1996.
16. Specifying Systems: The TLA+ Language and Tools for Hardware and Software Engineers, L. Lamport, Addison-Wesley, 2003.
17. Parallel Program Design: A Foundation, K.M. Chandy and J. Misra, Addison-Wesley, 1988.
18. A Discipline of Multiprogramming: Programming Theory for Distributed Applications, J. Misra, Springer, 2001
19. Beauty Is Our Business: A Birthday Salute to Edsger W. Dijkstra, Edited by W.H.J. Feijen, A.J.M. van Gasteren, D. Gries, and J. Misra, Springer-Verlag, 1990
20. The Formal Methods Page: http://vl.fmnet.info/, J. Bowen.
</td></tr>
<tr><td>評量方式</td><td>
<table>
<tr><th>No.</th><th>項目</th><th>百分比</th><th>說明</th></tr>
<tr><td>2.</td><td>期末考</td><td>40%</td><td></td></tr>
<tr><td>3.</td><td>作業</td><td>20%</td><td></td></tr>
<tr><td>4.</td><td>期末報告</td><td>40%</td><td></td></tr>
</table>
</td></tr>
</table>

週次	單元主題
第 1 週	Introduction, Propositional Logic
第 2 週	First-Order Logic
第 3 週	Logical Proofs in the Coq Proof Assistant
第 4 週	Verification of Sequential Programs: Hoare Logic
第 5 週	Verification of Sequential Programs: Soundness and Completeness of Hoare Logic
第 6 週	Predicate Transformers and Program Derivation
第 7 週	Semantic Modeling in Coq
第 8 週	Procedures + Object Orientation
第 9 週	Program Verification Tools: Why, Caduceus, and Krakatoa
第 10 週	Data Refinement + Formal Methods: Z
第 11 週	Data Refinement + Formal Methods: B
第 12 週	Data Refinement + Formal Methods: Alloy
第 13 週	Concurrent, Reactive Systems: Owicki-Gries Method
第 14 週	Concurrent, Reactive Systems: UNITY, Linear Temporal Logic
第 15 週	Selected Topics: Modular/Compositional Reasoning
第 16 週	Final
第 17 週	Selected Topics: Separation Logic
第 18 週	Selected Topics: Proof-Carrying Code