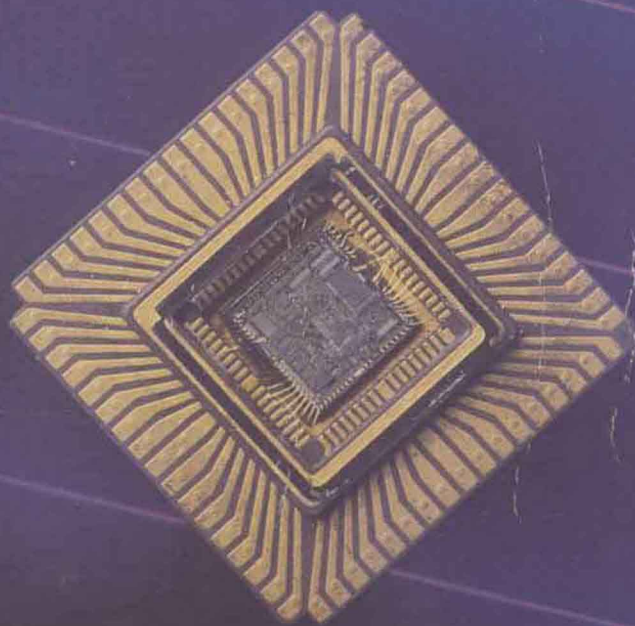


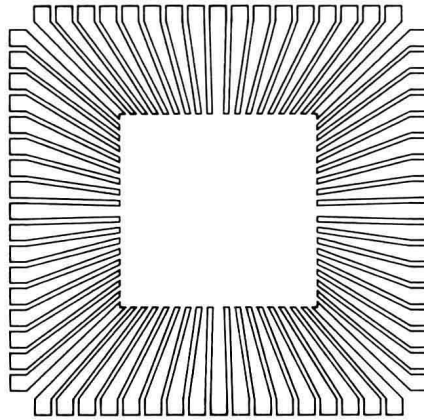
S
Y
B
E
X

PROGRAMMING THE 80286

C. Vieillefond



PROGRAMMING THE 80286



C. Vieillefond



SAN FRANCISCO • PARIS • DÜSSELDORF • LONDON

English translation by Idem Translation Center, San Francisco, CA
Book design by Jeffrey James Giese
Cover design by Thomas Ingalls + Associates

80286, 80287, 8086, 8259, 8282, 8283, 8286, 8287, 82284, 82286, and 82289 are trademarks of Intel Corporation. All mnemonics copyright Intel Corporation. Technical illustrations reproduced by permission of Intel Corporation, copyright 1983.

Macro Assembler is a trademark of Microsoft Corporation.
SYBEX is a registered trademark of SYBEX, Inc.

SYBEX is not affiliated with any manufacturer.

Every effort has been made to supply complete and accurate information. However, SYBEX assumes no responsibility for its use, nor for any infringements of patents or other rights of third parties which would result.

Copyright ©1987 SYBEX Inc., 2021 Challenger Drive #100, Alameda, CA 94501. World rights reserved. No part of this publication may be stored in a retrieval system, transmitted, or reproduced in any way, including but not limited to photocopy, photograph, magnetic or other record, without the prior agreement and written permission of the publisher.

Library of Congress Card Number: 87-60803
ISBN 0-89588-277-9
Manufactured in the United States of America
10 9 8 7 6 5 4 3 2 1

Originally published in French as *Mise en Oeuvre de l'iAPX 286* © 1986 Sybex-Europe.

PROGRAMMING THE 80286



ACKNOWLEDGMENTS

First, thanks must go to M. Delemarre, who provided the impetus for this book and put at my disposal all of the tools necessary for its realization. I am equally grateful to M. Crowitz, for being available when needed, and for his excellent and efficacious collaboration.

Finally, I warmly thank E. Bost and Francois Retaureau, who gave me permission to use certain technical information and thus participated in the creation of *Programming the 80286*.

—C. V.

Thanks are also owed to the following people, who contributed to the American edition of this book: Mich Aoki, of Idem Translation Center, for valuable suggestions beyond the scope of a simple translation; Greg Hooten and Joel Kroman for technical review and assistance; Olivia Shinomoto for word processing; Cheryl Vega for typesetting; Gwenyth Swain and Aidan Wylde for proofreading; Jim Compton for editing; Suzy Anger, Bret Rohmer, and Karl Ray for coordinating and scheduling; and R. S. Langer for advice and encouragement.

INTRODUCTION

The study of a microprocessor would be incomplete without an in-depth examination of both its physical structure and its processing capabilities. For this reason, this book explores all of the characteristics of the 80286: both hardware and software.

The purpose of any book about a microprocessor is to bring to light its essential mechanisms, using examples, and to define the major characteristics of the chip. Ultimately, it is to achieve deeper insight into the microprocessor's potential and purpose.

Programming the 80286 begins by probing the hardware features of the processor and its environment.

The first chapters are intended to enable anyone wishing to design a basic board for the 80286 to map out the configuration requirements of a minimal system quickly and easily.

Therefore, this section is addressed to technicians, research engineers, designers, and anyone desiring to implement the 80286 chip into a board design.

Next, the book presents the software capabilities of this processor and demonstrates its structural orientation—the operating system.

I would like to stress that the presentation of all the processing mechanisms—memory management, multitasking, and privilege levels (which are basic concepts of all operating systems) is intended to be purely educational. These chapters are written for persons working on the software: development engineers, students, and users who want to optimize the powers of this processor.

Diagrams and flowcharts are used to illustrate and reinforce the various concepts presented. Exercises are provided at the end of most chapters to enable readers to retain the major points discussed and test their comprehension.

This book assumes the reader is familiar with the basic theory of microprocessors (the structure of a central processing unit, the concept of interrupts, and so on). On the other hand, it is written in such a way that the reader can quickly cover the ground between the 8086 and the 80286, as each new feature is presented.

With regard to the implementation and execution of the programs, you will need only an 80286-based system supporting either the Microsoft Macro Assembler under a DOS operating system or the Intel 286 development system.

HOW TO USE THIS BOOK

The following summarizes each chapter of this book.

Chapter 1—Overview of the 80286 Microprocessor: This chapter describes the input and output signals of the 80286. It presents the CPU's internal registers and the structure of the status flag register.

Chapter 2—80286 System Architecture: This chapter places the 80286 in its environment. It discusses the role of the 82284 clock generator and the 82288 bus controller, and it describes the interface between the CPU and peripheral circuits in its discussion of the read and write bus cycles.

Chapter 3—Memory Management and Virtual Addressing: This chapter introduces the advanced memory management features of the 80286. The concepts presented include memory segmentation; virtual addressing; virtual-to-physical address translation; descriptor tables; data, code, and system segment descriptors; and memory management registers.

The material in this chapter is essential to understanding the structure of the 80286.

Chapter 4—Protection: This chapter describes the 80286's protection mechanisms. It explains the notion of privilege levels and shows how gates are used to implement these levels.

It is important to understand the underlying principle of the gate and its role in ensuring data integrity.

Chapter 5—Task Switching: This chapter explains the basics of task switching, the data structures used to ensure proper task isolation, the task status segment, task gates, and interrupt tasks.

Chapter 6—Interrupts: This chapter examines the software characteristics of interrupts. Topics discussed include the interrupt descriptor table, interrupt and trap gates, real-address mode interrupts, maskable interrupts and non-maskable interrupts.

Chapter 7—System Initialization: This chapter explains the principle of system initialization in real-address mode and in protected mode.

Chapter 8—Programming the 80286: This chapter introduces the various addressing modes used by the 80286 and summarizes the instruction set as well as the basic tools used in program development.

Chapter 9—The Instruction Set: This chapter presents the 80286 instruction set. The instructions are organized alphabetically according to their function.

Chapter 10—Sample Programs: This chapter contains program examples intended to illustrate the concepts presented in earlier chapters. Programs 1 to 11 are examples of using the 80286 instruction set. Program 12 is an example of CPU dialog with the 80287 numeric coprocessor. Program 14 implements the task switching mechanism. Program 15 demonstrates the role of the ENTER and LEAVE instructions.

Appendix A—The Build File Format: This appendix presents the syntax of the build files needed to run the program examples.

Appendix B—Exceptions in Protected Mode: This appendix summarizes the protected-mode exceptions to the CALL, INT, INTO, IRET, JMP, LDS, LES, MOV, POP, and RET instructions.

OVERVIEW OF THE 80286 MICROPROCESSOR

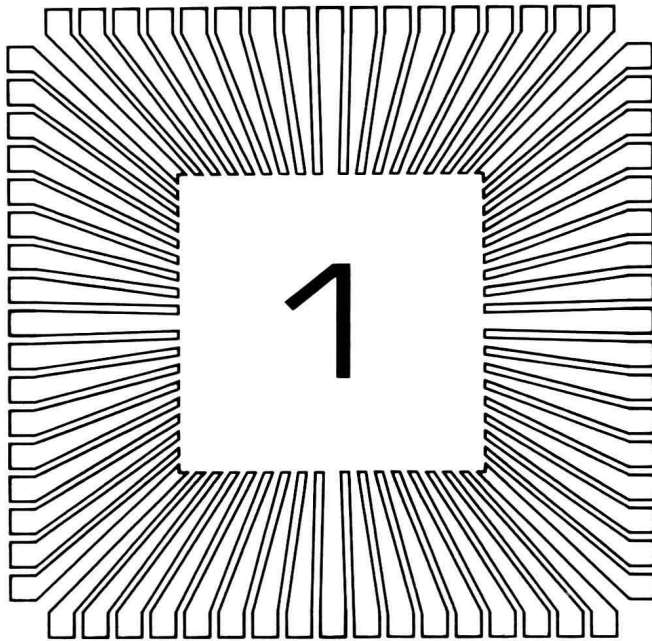


TABLE OF CONTENTS

Introduction	xx
Chapter 1: Overview of the 80286 Microprocessor	1
Introduction	1
80286 Modes of Operation	1
80286 Signals	2
System Clock Input (CLK)	2
System Power (V_{CC}) and System Ground (V_{SS})	3
The CAP Pin	4
Data Bus Signals (D0–D15)	5
Address Bus Outputs (A0–A23)	5
Bus High Enable Output (\overline{BHE})	6
Memory/IO Selection Output (M/\overline{IO})	7
Code/Interrupt Acknowledge Output (COD/\overline{INTA})	9
Bus Cycle Status Outputs ($\overline{S1}$, $\overline{S0}$)	9
Bus Ready Input (\overline{READY})	10
Interrupt Request Input (\overline{INTR})	11
Non-Maskable Interrupt Request Input (\overline{NMI})	12
Bus Hold Request and Hold Acknowledge Signals (HOLD Input, HLDA Output)	12
Bus Lock Output (\overline{LOCK})	12
Processor Extension Operand Request and Acknowledge Signals (\overline{PEREQ} Input, \overline{PEACK} Output)	13
Processor Extension Control Inputs (\overline{BUSY} , \overline{ERROR})	13
System Reset Input (RESET)	13
80286 Processor Architecture	14
Bus Unit (BU)	14
Instruction Unit (IU)	15
Execution Unit (EU)	15
Address Unit (AU)	15

80286 Internal Registers	16
General Registers	16
Segment Registers	17
Status and Control Registers	18

Chapter 2: 80286 System Architecture	25
Introduction	25
Bus Organization	25
System Cycles	27
System Clock Cycle (CLK)	28
Processor Clock Cycle (PCLK)	28
Bus Cycle	29
Instruction Cycle	29
The 82284 Clock Generator	29
The 82288 Bus Controller	38
Memory Read/Write Command Outputs ($\overline{\text{MRDC}}$, $\overline{\text{MWTC}}$)	38
Command Enable Latch Input (CENL)	38
Multibus Control Input (MB)	39
Address Latch Enable Output (ALE)	40
Command Delay Input (CMDLY)	40
Command Enable/Address Enable Input (CEN/ $\overline{\text{AEN}}$)	45
80286 Bus Cycles	46
Read Cycle	47
Write Cycle	49
80286 Interrupt Organization	51
Nonmaskable Interrupt Request [NMI]	52
Interrupt Request Input [INTR]	53
Interrupt Acknowledge Bus	

Sequence	53
80286 Bus Control Signals	56
80286 Memory Interfacing	58
 Chapter 3: Memory Management and Virtual Addressing	 67
Introduction	67
Memory Segmentation	67
Virtual Address Structure	69
Virtual-to-Physical Address Translation	70
Descriptor Tables	71
Data Segment Descriptors	73
Executable Code Segment Descriptors	77
System Segment Descriptors	79
Memory Management Registers	80
Segment Registers CS, DS, ES, and SS	81
GDTR and LDTR Registers	83
Summary	86
Exercises	89
Questions	89
Answers	91
 Chapter 4: Protection	 95
Introduction	95
Privilege Levels	95
DPL, CPL, RPL, and EPL	97
DPL—Descriptor Privilege Level	97
CPL—Current Privilege Level	97

RPL—Requested Privilege Level	97
EPL—Effective Privilege Level	98
Accessing Data Segments	98
Accessing Code Segments	99
Gates	100
Call Gates	103
Stack Organization	104
Parameter Passing	106
Privilege Restrictions	108
Conforming Code Segments	108
Privilege Restrictions Using RPL and EPL	109
ARPL (Adjust RPL)	110
Privileged and Trusted Instructions	112
Privileged Instructions	112
Trusted Instructions	113
Aliases	114
Summary	116
Exercises	116
Questions	116
Answers	118
 Chapter 5: Task Switching	 121
Introduction	121
The Task State Segment	121
Task Switching	123
What Happens During Task Switching	128
Task Gates and Interrupt Tasks	128
Summary	133

Exercises	133
Questions	133
Answers	134

Chapter 6: Interrupts and Exceptions 139

Introduction	139
Gate Descriptors	139
Interrupt Descriptor Table	140
Interrupt and Trap Gates	141
Reserved Exceptions and Interrupts	145
Divide Error—Interrupt 0 (Vector 0)	145
Single-Step—Interrupt 1 (Vector 1)	145
NMI (Non-Maskable Interrupt)—Interrupt 2 (Vector 2)	146
Breakpoint—Interrupt 3 (Vector 3)	146
Overflow—Interrupt 4 (Vector 4)	147
Bound Check—Interrupt 5 (Vector 5)	147
Invalid Opcode (UD)—Interrupt 6 (Vector 6)	147
Processor Extension Not Available (NM)— Interrupt 7 (Vector 7)	147
Double Fault (DF)—Interrupt 8 (Vector 8)	148
Processor Extension Segment Overrun— Interrupt 9 (Vector 9)	149
Invalid Task State Segment (TS)— Interrupt 10 (Vector 10)	149
Segment Not Present (NP)—Interrupt 11 (Vector 11)	149
Stack Fault (SS)—Interrupt 12 (Vector 12)	150
General Protection Fault (GP)—Interrupt 13 (Vector 13)	150
Processor Extension Error (MF)— Interrupt 16 (Vector 16)	150
Real Address Mode Interrupts	151
Interrupt Table Limit Too Small—Interrupt 8 (Vector 8)	151

Vectors 10, 11, and 12	152
Segment Overrun—Interrupt 13 (Vector 13)	152
Summary	152
Exercises	153
Questions	153
Answers	153

Chapter 7: System Initialization 157

Initial Processor State	157
Real Address Mode Initialization	159
Protected Mode Initialization	159

Chapter 8: Programming the 80286 163

Addressing Modes	163
Register and Immediate Addressing Modes	163
Memory Addressing Modes	164
80286 Instructions	169
Data Transfer Instructions	171
String Instructions	171
Arithmetic Instructions	171
Logical Instructions	172
Control Transfer Instructions	173
Processor Control Instructions	174
High-Level Instructions	175
80286 Development Tools	176
ASM286	177
Structure of an 80286 Assembly Language	
Source Module	177
Segment Definition	178
Procedure Definition	178

BND286	179
BLD286	179

Chapter 9: The 80286 Instruction Set	183
Instruction Mnemonic	183
Functional Description of an Instruction	184
Flags	185
Exceptions	185
Identifiers	185
Execution Time	186
Instruction Format	187
Basic Instruction Formats	188
AAA	190
AAD	192
AAM	193
AAS	194
ADC	196
ADD	198
AND	200
ARPL	202
BOUND	204
CALL	206
CBW	210
CLC	211
CLD	212

CLI	213
CLTS	214
CMC	215
CMP	216
CMPS/CMPSB/CMPSW	218
CWD	220
DAA	221
DAS	223
DEC	225
DIV	226
ENTER	228
HLT	230
IDIV	231
IMUL	233
IN	235
INC	236
INS/INSB/INSW	237
INT	239
INTO	241
IRET	242
<i>Jcond</i>	244
JMP	247
LAHF	250
LAR	251
LDS/LES	253
LEA	255
LEAVE	256
LGDT/LIDT	257