

Contents

*“Far better an approximate answer to the right question,
which is often vague, than an exact answer to the wrong question,
which can always be made precise.”
(John Tukey, 1915–2000)*

Preface	v	
List of Figures	ix	
List of Tables	xi	
1	Getting Started	1
1.1	Installation	2
1.2	How it Works	3
1.2.1	Tokenization	3
1.2.2	General Browsing	8
1.2.3	Query Libraries	11
1.3	Query Types	13
1.3.1	Interactive Queries	13
1.3.2	Pattern Matching	15
1.3.3	Inline Programs	17
1.3.4	Standalone Checkers	19
1.4	Using Parallelism	20
2	Interactive Queries	22
2.1	Mark, Reset, and Display	23
2.2	Ncore	27
2.3	Undo	28
2.4	Requires	28

2.5	Inspect	28
2.6	Fcts	29
2.7	Context	30
2.8	Finding Words in Strings	31
2.9	Finding Files that Include a Given File	32
2.10	Finding for-loops that Contain Assignments to <i>x</i>	34
2.11	Using Token Type References	35
2.12	Generating Code Statistics	36
2.13	Code, Comments, and Constraints	37
2.14	Finding Long Identifiers	38
2.15	Finding Nested Switch Statements	39
2.16	Finding Missing Default Clause	40
2.17	Saving and Restoring Matches	43
2.18	Command History	45
2.19	Finding Recursive Functions	45
2.20	Named Scripts with Parameters	48
2.21	Redirecting Output and Shell Escapes	49
2.22	Default Prompts	50
2.23	Language Extension	50
2.24	Command Qualifiers	51
	Exercises	56
3	Pattern Matching	57
3.1	Pattern Expressions	58
3.2	The Case of the Missing Default	59
3.3	Adding Bound Variables and Constraints	60
3.4	Finding Function Definitions	61
3.5	Interactive Use	63
3.6	Qualified Matches	64
3.7	Brace Pairing	65
3.8	The Algorithm (skip to pg. 71 on first reading)	66
3.9	Examples of Brace Pairing	68
3.10	Token Markings	70
3.11	Referencing Brace Levels	71
3.12	Choice and Negation	72
3.13	Operations on Pattern Sets	73
3.14	EOL and EOF	76
	Exercises	77
4	Inline Programs	78
4.1	Stop and Next	80
4.2	Token Attributes	80
4.3	Editing Token Attributes	82
4.4	Grammar	82
4.5	If-Then-Else	82
4.6	While: Iteration	84
4.7	Floating Point Variables	84
4.8	Foreach: Accessing Sets and Arrays	87

4.9	Associative Arrays	89
4.10	Operators and Expressions	93
4.11	Command-Line Arguments	95
4.12	Defining Functions	97
4.13	File I/O	98
4.14	Walkthrough of an Example	101
	Exercises	104
5	Using Concurrency	105
5.1	The Sum Function	106
5.2	Array Unification of Integer Values	109
5.3	Array Unification of Strings or Token References	110
5.4	Parallel Word Count	112
5.5	Classic Word Count	113
5.6	Using Predefined Variables	116
5.7	Sharing Files	116
5.8	The Sieve of Eratosthenes	117
5.9	A Simpler Way	120
5.10	Using Shared Memory	121
5.11	The Exec Function	122
	Exercises	124
6	Building Standalone Checkers	125
6.1	Basic Structure	125
6.2	Passing Command-Line Arguments	128
6.3	Some Example Checkers	128
6.4	A CWE Checker	130
6.5	Taint Analysis	131
6.6	Duplicate Detection	132
	Exercises	134
7	Graphical User Interface	135
7.1	Overview	136
7.2	Main Displays	137
7.3	Menus	141
7.3.1	File Menu	141
7.3.2	Find Menu	142
7.3.3	View Menu	143
7.3.4	Global Options	144
7.3.5	Defining Pattern Sets	144
7.4	Metrics Tab	146
7.5	Heatmap Tab	147
7.6	Warnings Tab	149
7.7	Help Tab	151
8	Runtime Verification	153
8.1	Using Streaming Input	153
8.2	Comparison with Existing Tools	154

8.3	Cobra Programs	154
8.4	Cobra Command Line	156
8.5	Results	157
	Exercises	159
9	Statistical Analysis	160
9.1	Inconsistent Use of Control Variables in For-Loops	161
9.2	Basic Method	163
9.3	Building a Reference Pattern Data-Set	164
9.4	Using the Reference Model to Analyze Code	168
9.5	Inconsistencies in the Use of Function Return Values	171
9.6	Inconsistencies in the Use of File Descriptors	173
9.7	Inconsistencies in the use of Lock Variables	175
9.8	Inconsistent Uses of snprintf	177
9.9	Synopsis	178
Reference Material		
A	Token Types	180
B	Token Attributes	181
C	Grammar for Inline Code	182
D	Predefined Inline Functions	188
E	Examples of Pattern Expressions	196
E.1	Finding Recursive Functions	196
E.2	MISRA 1997 Rule 62	197
E.3	MISRA 1997 Rule 55	198
E.4	MISRA 1997 Rule 36	198
E.5	MISRA 2012 Rule 2.6	199
E.6	CWE 119	199
E.7	For-loops that Modify the Control Variable in the Body	200
E.8	For-loops that Contain Calls to Emalloc	200
E.9	Combining Results	200
E.10	More Challenging Cases	203
E.11	Failure to Close	204
F	Examples of Regular Expressions	208
G	Answers to Exercises	210
Index		219-225