The Correctness-by-Construction Approach to Programming

- Step-by-step explanation of how to derive mathematically correct algorithms using small and tractable refinements
- Detailed illustration of the presented methodology through a set of carefully selected graded examples
- Practical applicability demonstrated by deriving non-trivial algorithms (e.g. in computational geometry) and algorithm taxonomies (as a basis for toolkit construction)

The focus of this book is on bridging the gap between two extreme methods for developing software. On the one hand, there are texts and approaches that are so formal that they scare off all but the most dedicated theoretical computer scientists. On the other, there are some who believe that any measure of formality is a waste of time, resulting in software that is developed by following gut feelings and intuitions. Kourie and Watson advocate an approach known as “correctness-by-construction,” a technique to derive algorithms that relies on formal theory, but that requires such theory to be deployed in a very systematic and pragmatic way. First they provide the key theoretical background (like first-order predicate logic or refinement laws) that is needed to understand and apply the method. They then detail a series of graded examples ranging from binary search to lattice cover graph construction and finite automata minimization in order to show how it can be applied to increasingly complex algorithmic problems. The principal purpose of this book is to change the way software developers approach their task at programming-in-the-small level, with a view to improving code quality. Thus it coheres with both the IEEE’s Guide to the Software Engineering Body of Knowledge (SWEBOK) recommendations, which identifies themes covered in this book as part of the software engineer’s arsenal of tools and methods, and with the goals of the Software Engineering Method and Theory (SEMAT) initiative, which aims to “refound software engineering based on a solid theory.”