Towards a Formal Verification of B+ Trees

Nicolai Dahl Blicher-Petersen, Christian Harrington, and Morten Fangel Jensen
{ndbl, cnha, mfan}@itu.dk

IT University of Copenhagen, Rued Langgaards Vej 7, 2300 Copenhagen S, Denmark

Abstract. The B+ tree data structure is a balanced, n-ary tree, used most often in databases and file systems. It is known for its high fanout, thereby minimizing the number of costly I/O operations. We implement a B+ tree in Gallina, along with insert and search functions. Using the Coq interactive proof assistant we define an inductive data type describing a valid B+ tree, as well as several other propositions. These are used to formally verify properties of the implemented insert and search functions, the last of which is formally proven correct. Furthermore, we state the elements needed for a complete formal proof of the insert function. We prove the most important element of these: that an inserted value can be found again. This is done through an intermediary proposition, letting us reason about insert and search independently.

Keywords: B+ tree, Coq, Gallina, Formal verification

1 Indexing

A Find Subtree Source