Verifying fileutils in ACL2: a case study

Mihir Parang Mehta

University of Texas at Austin, Department of Computer Science,
2317 Speedway, Austin, TX 78712, USA

Abstract. We describe an effort to verify the `fileutils` subset of the GNU `coreutils` against specifications built upon a verified model of the FAT32 filesystem.

Keywords: interactive theorem proving, filesystems

1 Introduction and overview

The `fileutils` are neat. They would be neater if formally verified.

2 Related work

Filesystem verification research has largely followed a pattern of synthesising a new filesystem based on a specification chosen for its ease in proving properties of interest, rather than similarity to an existing filesystem. FSCQ [1] is an example.

3 Evaluation

We specify and verify all the utilities in the `fileutils` subset of `coreutils`.

4 Conclusion

This work shows that a formal model of a single filesystem can be used to verify application programs with non-trivial interactions with the filesystem. Additionally, this work provides library support for working with additional filesystems and possibly identifying differences between different filesystems when used with the same program.

5 Future work

We hope to expand on this work by specifying and verifying the operation of application programs in multiprogramming environments where concurrent accesses to the filesystem may be made by different processes.

Acknowledgments. This material is based upon work supported by the National Science Foundation SaTC program under contract number CNS-1525472. Thanks are also due to Warren A. Hunt Jr. and Matthew J. Kaufmann for their guidance.

References

1. Chen, H., Ziegler, D., Chajed, T., Chlipala, A., Kaashoek, M.F., Zeldovich, N.: Using crash hoare logic for certifying the FSCQ file system. In: Gulati, A., Weatherspoon, H. (eds.) 2016 USENIX Annual Technical Conference, USENIX ATC 2016, Denver, CO, USA, June 22-24, 2016. USENIX Association (2016). https://doi.org/10.1145/2815400.2815402, `https://www.usenix.org/conference/atc16`