Corrections to Program Verification Rules

Zsolt Borsi, Tibor Gregorics

Department of Software Technology and Methodology
Faculty of Informatics
Eötvös Loránd University

{bzsr,gt}@inf.elte.hu

The subject of this paper is a program verification method that takes into account abortion caused by partial functions in program statements. In particular, boolean expressions of various statements will be investigated that are not well-defined. For example, a loop aborts if its execution begins in a state for which the loop condition is undefined. This work considers the program constructs of nondeterministic sequential programs and also deals with the synchronization statement of parallel programs introduced by Owicki and Gries [**?**].
The syntax of program constructs will be reviewed and their semantics will be formally defined in such a way that they suit the relational model of programming developed at Eötvös Loránd University [**?**, **?**, **?**]. This relational model defines the program as a set of its possible executions and also provides definition for other important programming notions like problem and solution.
The proof rules of total correctness [**?**, **?**, **?**, **?**, **?**] will be extended by treating abortion caused by partial functions. The use of these rules will be demonstrated by means of a verification case study.

References

[1] Dijkstra E.W.: *A Discipline of Programming*, Prentice-Hall, Englewood Cliffs, New York, 1976.

[2] Fóthi, Á.: *A Mathematical Approach to Programming*, Ann. Univ. Sci. Budapest. Sect. Comput. 9 (1988), 105-114.

[3] Fóthi Á.: *Bevezetés a programozáshoz*, ELTE Eötvös Kiadó. 2005. (in Hungarian)

[4] Fóthi, Á., Horváth, Z., Nyéky-Gaizler, J.: *A Relational Model of Transformation in Programming*, Proc. 3th International Conference on Applied Informatics, Eger-Noszvaj, Hungary, August 24-28. 1997.

[5] Gregorics, T.: *Concept of abstract program*, Acta Universitatis Sapientiae, Informatica, 4, 1 (2012), 7-16

[6] Gries, D.: *The Science of Programming*, Springer, Berlin, 1981.

[7] Hoare, C.A.: *An axiomatic basis for computer programming*, Comm. ACM 12, pp. 576-580 (1969)

[8] Krzysztof R. Apt, Ernst-Rdiger Olderog: *Verification of Sequential and Concurrent Program*, Springer-Verlag, 1997.

[9] S. Owicki, D. Gries: *An axiomatic proof technique for parallel programs*, Acta Inf., 6, pp. 319-340.

[10] Williem-Paul de Roever et al.: *Concurrency Verification*, Cambridge University Press, 2001.

[11] Workgroup on Relational Models of Programming - Fóthi Á. et al.: Some concepts of a Relational Model of Programming. Varga L., ed., *Proc. 4th Symposium on Programming Language and Software Tools*, Visegrád, Hungary, June 8-14, 1995, 434-446.