Szoftver hibatűrés vizsgálata formális ekvivalencia ellenőrzéssel

Zalán András, Matematikus szak IV. évf.

Konzulens: dr. Majzik István, Méréstechnika és Információs Rsz. Tsz.

Egyre több az olyan számítógépes alkalmazás, ahol fontos szempont a hibatűrés. Egy rendszer akkor hibatűrő, ha bizonyos hibák esetén is tudja nyújtani a felhasználó által elvárt szolgáltatásokat.

A számítógépes program tervezője több technikát is alkalmazhat a hibatűrés érdekében. Léteznek általánosan elterjedt módszerek (pl. ismételt végrehajtás, recovery blokk technika) illetve a tervező használhat alkalmazás-specifikus megoldásokat is. Mindkét esetben szükséges az alkalmazott megoldás helyességének igazolása: be kell látni, hogy a figyelembe vett hiba esetén sem érzékeli a felhasználó a szolgáltatás kimaradását, vagyis a hibatűrő rendszer viselkedése az adott hiba esetén ekvivalens a hibamentes rendszer viselkedésével.

A viselkedési ekvivalencia vizsgálatához rendelkezésre állnak kidolgozott ekvivalencia (pl. biszimuláció) illetve részben rendező relációk. Ezeket automatákra dolgozták ki. A tervező azonban rendszerint egy magasabb szintű modellező nyelvet használ. Objektum-orientált rendszerek esetén ilyen az UML.

Dolgozatomban megvizsgálom, hogy hogyan alkalmazhatók az ekvivalencia ellenőrzés formális módszerei UML nyelven leírt hibatűrő technikák esetén. Ennek célja kettős. Egyrészt így lehetővé válik egy modellkönyvtár (tervezési minta készlet) kidolgozása, amelyben általánosan használható, igazoltan helyes technikák szerepelnek. Másrészt pedig módszer adható arra, hogy alkalmazás-specifikus technikák ellenőrzése hogyan történhet meg.

A vizsgálat során kliens-szerver rendszerek UML modelljeit készítem el, ahol a rendszerben a szerver hibáját többféle stratégia szerint (pl. újrapróbálkozás, redundáns szerverek soros és párhuzamos végrehajtása) lehet elrejteni a felhasználó elől. Az UML osztálydiagram és állapottérkép diagram alapján felveszem a megfelelő működésű automatákat, és a hibatűrő rendszert leíró automata viselkedését a hibamentes referencia rendszernek megfelelő automata viselkedésével hasonlítom össze. Egyező viselkedés esetén igazolt az alkalmazott stratégia helyessége.