Kivonat

Kritikus rendszerek tervezésekor a helyes működés kulcsfontosságú: az esetleges tervezési hibák ilyenkor hatalmas anyagi kárt, vagy akár személyi sérüléssel járól baleseteket is okozhatnak. A hibamentesség a hagyományos tesztelési módszerekkel nem bizonyítható, ennek belátásához (vagy legalábbis közelítéséhez) a lehetséges viselkedések kimerítő vizsgálata szükséges. Ehhez adnak támogatást a különböző formális verifikációs módszerek, ahol a rendszereknek megfeleltetett tervezési modellek helyessége a matematikai precizitással belátható.

Az egyik ilyen módszer, a logikaalapú szimbolikus modellellenőrzés vezető technikája az ellenpélda-vezérelt absztrakció finomítás (Counterexample-Guided Abstraction Refinement, CEGAR). A módszer egyre finomabb absztrakciókon iterálva vizsgálja a modellt, ezzel elkerülve az irreleváns részek vizsgálatát. Predikátumabsztrakció használatakor az állapottér-felderítés során megoldandó az AllSAT-probléma, ahol a feladat egy adott logikai kifejezésre az összes őt igazzá tevő kiértékelés megtalálása. Ennek megoldására már állnak rendelkezésre AllSAT-megoldók, a kutatás célja az eddigieknél rugalmasabb, az alkalmazási terület igényei szerint testreszabható megoldó tervezése, amit sikerrel lehetne alkalmazni a különböző modellellenőrzési módszereken belül is.

Dolgozatomban egy olyan megoldást javaslok, ahol az AllSAT megoldóknál sokkal kiforrottabb és szélesebb körben elérhető SAT/SMT megoldók felhasználásával a megoldásokat döntési diagram strukturába szervezem, és ez a struktúra nem csak a kompakt tárolást, hanem a megoldások lekérdezésének vezérlését is végzi. Várható, hogy a megoldás a modellellenőrzőkben jelenleg használt módszerhez képest versenyképes lesz, emellett a funkciókör bővítése szélesebb körű alkalmazhatósághoz vezethet. Fontos kiterjesztés, hogy a módszer nem csak SAT, de SMT megoldókkal is működik, tehát a változók nem csak bináris értékűek lehetnek. Dolgozatomban kitérek az emiatt felmerülő új kihívásokra, és ezekre a különböző felhasználási területek igényeihez igazodó megoldásokat javaslok. A módszert implementálom egy konfigurálható modellellenőrző keretrendszerben, integrálom már létező algoritmusokkal, és teljesítményét mérésekkel vizsgálom.