Jedním ze způsobů prevence chyb v objektově orientovaných programech je používání kontraktů, kterými jsou například vstupní a výstupní podmínky metod nebo invarianty tříd. Ve frameworku .NET je používání kontraktů umožněno díky frameworku Code Contracts, který mimo jiné obsahuje nástroj Clousot na statickou analýzu programů, založený na abstraktní interpretaci.
Ačkoli řetězce jsou jedním ze základních typů v programech pro .NET, Clousot neobsahuje použitelnou podporu pro analýzu řetězcových hodnot.
V této práci probereme specifika práce s řetězci v jazyce C# a frameworku .NET a ukážeme, jak je možné ji pokrýt statickou analýzou. Zvolený přístup využívá metody třídy String a omezenou podmnožinu regulárních výrazů ke specifikaci vlastností řetězců v kódu, a abstraktní interpretaci s nerelačními abstraktními doménami k důkazům těchto vlastností.
Zvolili jsme několik již publikovaných abstraktních domén pro řetězce, které se mezi sebou liší složitostí a schopností reprezentovat různé vlastnosti řetězců. Tyto domény jsme adaptovali pro zvolené prostředí, což zahrnovalo definici abstraktní sémantiky pro podporované řetězcové operace. Abstraktní domény jsme implementovali v nástroji Clousot, a to tak, aby bylo v budoucnu možné rozšíření o další domény.