Specyfikacja projektu dekompilatora

Autorzy: Aleksander Balicki, Łukasz Zapart

March 9, 2010

1 Specyfikacja zadania

1.1 Opis zadania

Napisać program dekompilujący programy do C, to jest, zamieniający kod maszynowy na kod w języku C.

1.2 Funkcjonalność

Program powinien być w stanie produkować kompilowalny kod w C zachowujący się jak wejściowy kod maszynowy. Program powinien też starać się produkować kod jak najbardziej czytelny dla człowieka, toteż powinien próbować rozpoznawać sygnatury funkcji, typy zmiennych, itd (probować, ponieważ te problemy są nieroztrzygalne).

1.3 Struktura

Struktura programu będzie się składać co najmniej z:

- deasemblera
- "parsera" asemblera do abstrakcyjnego drzewa rozbioru
- generator kodu z drzewa rozbioru do C

1.4 Planowana technologia

Program będzie napisany w Pythonie i będzie udostępniony publicznie na licencji MIT.

2 Harmonogram pracy

Harmonogram pracy podzielony jest na pięć 3-tygodniowych bloków.

2.1 Blok 1.

- Deasembler do tokenów (AB, ŁZ).
- Postawienie traq i ewentualne postawienie svn (chyba, że wybierzemy git) (AB).

2.2 Blok 2.

Generator kodu "1-1", czyli kodu w C, który znaczy to samo, co kod maszynowy, ale na którym nie zostały wykonane żadne transformacje związane ze zwiększeniem czytelności kodu. (AB, ŁZ).

2.3 Blok 3.

Parser tokenów do abstrakcyjnego drzewa rozbioru. (AB, ŁZ).

2.4 Blok 4.

Dodanie funkcjonalności zwiększającej czytelność kodu (rozpoznawanie sygnatur, typów, pętli, struktur tam gdzie to możliwe) (AB, ŁZ).

2.5 Blok 5.

Testowanie kodu przez innych użytkowników oraz reakcja na ich uwagi (AB, ŁZ).