نقش و کاربرد گرامرهای ویژه در مهندسی معکوس نرم افزار

تمرین درس کامپایلر پیشرفته

دانشجو:

محسن امیریان ۹۵۷۲۳۰۳٤

استاد:

دکتر سعید پارسا

مهر ماه ۱۳۹۵

مهندسی معکوس

مهندسی معکوس به طور عمده در استفاده‌های تجاری و نظامی به کار می‌رود و هدف آن استنباط پارامترهای طراحی یک محصول موجود بدون داشتن دانش کافی در زمینه تولید آن محصول و فقط با پیمودن فرآیند معکوس و به کارگیری تکنیک‌های مشابه می‌باشد.

در عمل دو نوع عمده از مهندسی معکوس وجود دارد. در حالت اول، سورس کد برای برنامه وجود دارد، اما سطوح بالاتری از جنبه های این برنامه، شاید مستندات ضعیف یا مستنداتی که دیگر اعتبار ندارد، مشاهده می شوند.در حالت دوم ، سورس کدی برای برنامه موجود نیست و هرگونه تلاشی در جهت استخراج یک سورس کد ممکن برای نرم افزار به عنوان مهندسی معکوس در نظر گرفته شده است.

مهندسی معکوس نرم افزار از روش های گوناگونی می تواند بدست آید. یکی از این روش ها دستیابی به سورس کد با استفاده از یک دیکامپایل کننده، فرایندی که تلاش می کند سورس کد را در بعضی زبان های سطح بالا برای برنامه ای که فقط در حالت بایت کد یا کدهای ماشین است فراهم کند.

گرامرهای ویژه

گرامرهای ویژه یک رسمی برای تعریف ویژگی برای تولیدات گرامر و مرتبط ساختن این ویژگی ها به مقادیر است. این ارزیابی ها در هنگامی که کامپایلر در حال پردازش کد است، در گره های درخت تجزیه نحوی رخ می دهد.

گرامر های ویژه همچنین می توانند برای ترجمه مستقیم درخت نحوی به کد قابل اجرا بر روی برخی از ماشین ها و یا به برخی زبان های میانی مورد استفاده قرار گیرند.

یکی از نقاط قدرت این گرامرها این است که می توانند به شیوه ای رسمی[1] اطلاعاتی را از هر جایی در درخت خلاصه نحوی به هر جای دیگری انتقال دهند.

گرامر ویژه به طور کلی به دو شکل در کامپایلر استفاده می شوند. یکی در ایجاد صفات مربوط به آزمون نوع در فاز تحلیل معنایی برنامه و دیگری ایجاد صفات لازم برای تولید کد در مرحله تحلیل نحوی (ترجمه هدایت شده یا مبتنی بر دستور). البته این فاز ها معمولا همزمان انجام می پذیرد. به عبارت ساده در گرامرهای ویژه برای هر غیرپایانه یا متغیر میانی یک صفت از جنس رشته در نظر گرفته می شود که محتوای آن حاوی کدی است که برای متغیر میانی ایجاد می شود.

کاربرد گرامرهای ویژه در صنعت

گرامرهای علاوه بر مطالعات آکادمیک، در حوزه ی کارهای صنعتی نیز کاربرد دارند که اما به این جنبه توجه کمتری شده است زیرا اغلب افراد درحوزه کامپیوتر از آن بی اطلاع هستند.

نمونه ای از گرامر ویژه ساخت درخت تجزیه نحوی در C++:

مثال زیر یک نمونه از کاربرد گرامرهای ویژه روی گرامر زبان C++ را نشان می دهد. دو صفت در قواعد این گرامر محاسبه می شوند. صفت tree که برای ساخت درخت تحلیل نحوی به کار می رود. صفت type که نوع هر عبارت را محاسبه می کند.

[1] Formal

```
postfix_expression = <
        = primary_expression .
        = p:postfix_expression '[' e:expression ']'
        { type := type_op (p:type, karray);
          tree := msubscript_expr ('[':Position, p:tree, e:tree); } .
        = postfix_expression '(' expression_list ')'
        { type := type_op (postfix_expression:type, kfunction);
          tree := mcall_expr ('(':Position, postfix_expression:tree,
                ReverseTree (expression_list:tree)); } .
        = s:simple_type_specifier '(' expression_list ')'
        { type := get_type (s:tree);
          tree := (s:tree->specifier.next = mnospecifier (),
                mconstruct_expr ('(':Position, s:tree,
                ReverseTree (expression_list:tree))); } .
        = ...
```

نتیجه گیری

مبحث گرامرهای ویژه و استفاده از آن ها، تا به امروز غالباً بصورت مطالعات آکادمیک مورد بررسی قرار گرفته اند. استفاده از آن ها در صنعت و به خصوص در مهندسی معکوس نرم افزار کمتر مورد توجه قرار گرفته است. از طرف دیگر روش های استفاده از گرامرهای ویژه در مهندسی معکوس نرم افزار فاقد ابزارهای شناخته شده و قدرتمند است که این موضوع ورود به این حوزه ی استفاده از گرامرهای ویژه را تا حدودی با دشواری مواجه کرده است.

اما با تمام این اوصاف از آنجایی که می توان به کد اکثر برنامه های کاربردی دسترسی پیدا کرد، داشتن توان مهندسی معکوس می تواند اطلاعات سودمندی از برنامه ها را بیرون کشیده و در اختیار ما قرار دهد که این اطلاعات در زمینه های مختلفی (ساخت نرم افزار مشابه با امکانات بیشتر، شناسایی ویروس ها و ساخت نمونه قدرتمند تر،...) قابل استفاده اند.