Entre los lenguajes de alto nivel y el código de máquina

Construcción de un compilador de PL/0 para Win32

Introducción

En este curso desarrollaremos un compilador para el lenguaje de programación PL/0, presentando una introducción general de la estructura y operación de los compiladores.

1. Comentarios generales sobre la teoría de compiladores

El diseño de programas para resolver problemas complejos es mucho más sencillo utilizando *lenguajes de alto nivel*, ya que se requieren menos conocimientos sobre la estructura interna del computador, aunque es obvio que éste sólo entiende el *código de máquina*. Por lo tanto, para que un computador pueda ejecutar programas escritos en un lenguaje de alto nivel, éstos deben ser traducidos a código de máquina. A este proceso se lo denomina *compilación*, y la herramienta que la lleva a cabo se llama *compilador*. Por ende, los compiladores son fundamentales para la computación, y su importancia se mantendrá en el futuro.

La entrada del compilador es el *código fuente*, es decir, el programa escrito en un lenguaje de alto nivel. El compilador analiza esta entrada y genera a su salida el *código objeto*. Existen distintas formas de código objeto, siendo una de las diferencias más destacables la que existe entre el código absoluto (el código de máquina con direcciones de memoria absolutas) y el código relocalizable (el código de máquina con desplazamientos de direcciones, y por lo tanto enlazable con otros módulos compilados por separado).

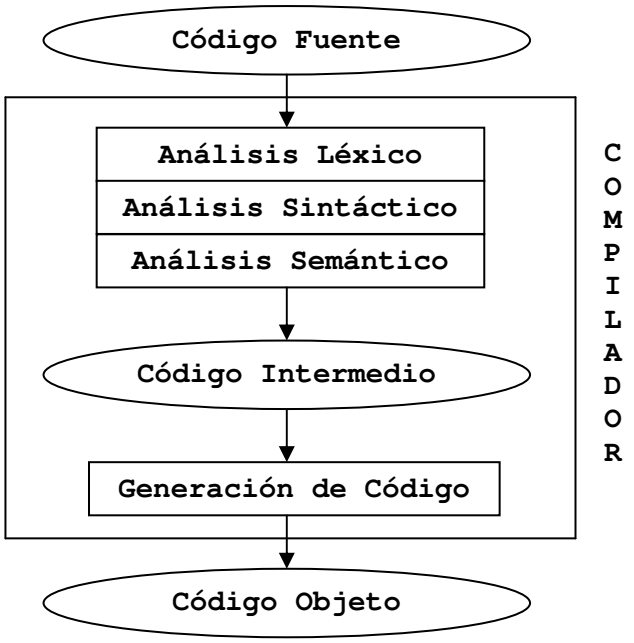
De acuerdo con los diferentes tipos de código y las diversas formas de funcionamiento, podemos distinguir entre los siguientes tipos de sistemas de compilación:

- Ensamblador: Traduce programas escritos en lenguaje ensamblador a código de máquina. El lenguaje ensamblador se caracteriza por el uso de mnemónicos para representar instrucciones y direcciones de memoria.
- Compilador: Traduce programas escritos en un lenguaje de alto nivel a código intermedio o a código de máquina. El código intermedio puede ser, por ejemplo, un lenguaje ensamblador o alguna otra forma de representación intermedia.

❒ **Intérprete: No genera código objeto, sino que analiza y ejecuta directamente cada sentencia del código fuente. Como no se genera código de máquina, en cierta forma los programas escritos para ser interpretados son independientes de la máquina.**

❒ **Preprocesador: Reemplaza macros, incluye archivos o extiende el lenguaje.**

En este curso sólo haremos hincapié en los compiladores, y estudiaremos las distintas fases del proceso de compilación, pero no nos detendremos en cuestiones marginales como los sistemas de edición y depuración que forman parte de todo ambiente de compilación moderno.



El análisis léxico es llevado a cabo por el analizador léxico (*lexical scanner* o simplemente *scanner*) y consiste en reconocer los componentes léxicos (símbolos del lenguaje) contenidos en el código fuente del programa a compilar, que ingresa como un flujo de caracteres.

El análisis sintáctico tiene como objetivo revisar si los símbolos detectados durante el análisis léxico aparecen en el orden correcto como para constituir un programa válido. El analizador sintáctico se conoce usualmente como *parser*.

El análisis semántico reconoce si las unidades gramaticales tienen sentido, detectando errores como inconsistencia de tipos u operaciones con objetos no declarados.

Finalmente, la generación de código es llevada a cabo por un módulo que usualmente es reemplazable, con lo cual se pueden obtener códigos objeto para distintas plataformas a partir de un mismo código intermedio. Además, hoy en día es común que compiladores de distintos lenguajes generen el mismo código intermedio, por lo que un programa ejecutable puede obtenerse enlazando módulos de código objeto obtenidos a partir de códigos fuente escritos en lenguajes distintos.

2. Estructura de los lenguajes

Los lenguajes se basan en un *vocabulario*. Sus elementos son comúnmente llamados *palabras*, pero en el estudio de los lenguajes formales se los denomina *símbolos*.

Es característico de los lenguajes que algunas secuencias de palabras sean reconocidas como *frases* correctas y otras no. Lo que determina si una secuencia de palabras es una frase correcta (o no) es la gramática, sintaxis o estructura del lenguaje. De hecho, definimos *sintaxis* como el conjunto de reglas que definen el conjunto de frases formalmente correctas.

Dado que la sintaxis provee a las frases de una estructura que nos sirve para reconocerles el significado, queda claro que la sintaxis y la *semántica* (el significado) están íntimamente conectados. Sin embargo, en un primer momento vamos a dedicarnos exclusivamente al estudio de la sintaxis.

Tomemos la frase "Martín duerme." La palabra "Martín" es el sujeto y la palabra "duerme" es el predicado. Esta frase pertenece a un lenguaje que puede, por ejemplo, estar definido por la siguiente sintaxis:

```
<frase> ::= <sujeto> <predicado>
<sujeto> ::= Martín | Julieta
<predicado> ::= duerme | juega
```

El significado de estas tres líneas es el siguiente:

1. **Una frase está formada por un sujeto seguido de un predicado.**
2. **El sujeto puede ser la palabra "Martín" o la palabra "Julieta"**
3. **El predicado puede ser la palabra "duerme" o la palabra "juega"**

Las frases correctas pueden derivarse a partir del *símbolo inicial* <frase> mediante la aplicación reiterada de *reglas de sustitución*.

La notación utilizada para escribir estas reglas se denomina BNF.

Las palabras *Martín*, *Julieta*, *duerme* y *juega* se denominan *símbolos terminales*. Una secuencia nula de símbolos se representa con ∈.

<frase>, <sujeto> y <predicado> son los *símbolos no terminales*. Las reglas se denominan *producciones*, ya que determinan cómo se pueden generar o *producir* frases correctas.

Los símbolos ::= y | se denominan metasímbolos de la notación BNF, y se pronuncian "puede sustituirse por" y "o", respectivamente. Aunque no forman parte de BNF (ya que son una extensión del mismo), también son consideradas metasímbolos las llaves { y } para encerrar símbolos que se repiten cero o más veces.

A veces, es posible simplificar la notación, utilizando letras minúsculas para los símbolos terminales y letras mayúsculas para los símbolos no terminales, en lugar de distinguirlos con < y >.

Ejemplo 1

S ::= AB

A ::= x|y

B ::= z|w

El lenguaje definido por esta sintaxis (que es equivalente a la sintaxis dada en la página anterior) es el compuesto por las cuatro frases *xz*, *yz*, *xw*, *yw*.

A diferencia del lenguaje anterior, el definido por la siguiente sintaxis está compuesto por un número infinito de frases:

Ejemplo 2

S ::= xA

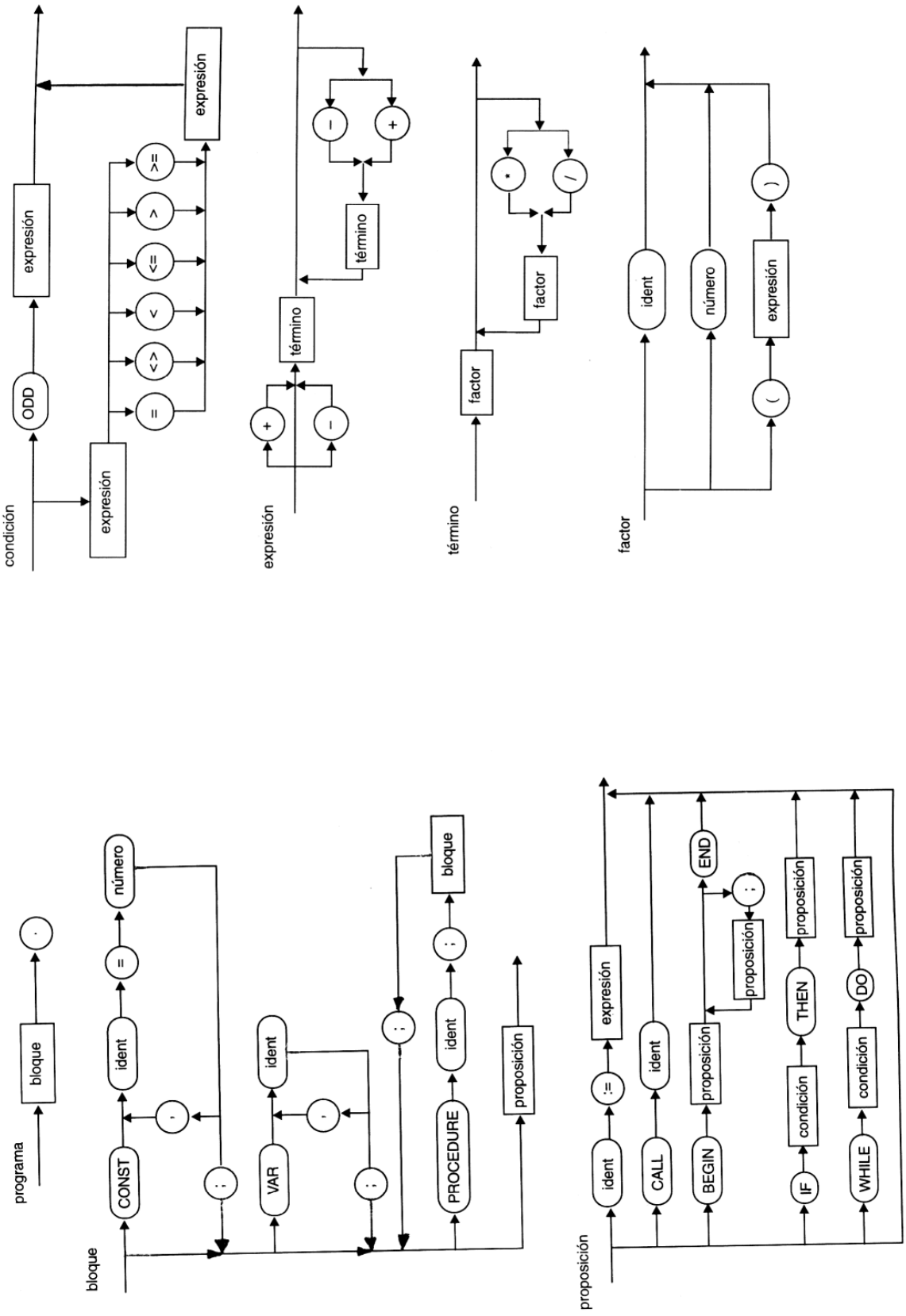
A ::= z|yA

A partir del símbolo inicial *S* pueden generarse las frases *xz*, *xyz*, *xyyz*, *xyyyz*, *xyyyyz*, ...

En síntesis, un lenguaje *L* se caracterizará con referencia a una gramática *G (T, N, P, S)*, donde:

- **❒ *T* es el conjunto de símbolos terminales**
- **❒ *N* es el conjunto de símbolos no terminales**
- **❒ *P* es el conjunto de producciones**
- **❒ *S* es el símbolo inicial (debe ser un símbolo no terminal)**

3. El lenguaje de programación PL/0



Ejemplo de programa escrito en PL/0

```
const M = 7, N = 85;
var X, Y, Z, Q, R;

procedure MULTIPLICAR;
var A, B;
begin
  A := X;
  B := Y;
  Z := 0;
  while B > 0 do
    begin
      if odd B then Z := Z + A;
      A := A * 2;
      B := B / 2
    end
end;

procedure DIVIDIR;
var W;
begin
  R := X;
  Q := 0;
  W := Y;
  while W <= R do W := W * 2;
  while W > Y do
    begin
      Q := Q * 2;
      W := W / 2;
      if W <= R then
        begin
          R := R - W;
          Q := Q + 1
        end
    end
end;

procedure MCD;
var F, G;
begin
  F := X;
  G := Y;
  while F <> G do
    begin
      if F < G then G := G - F;
      if G < F then F := F - G
    end;
  Z := F
end;

begin
  X := M;  Y := N;  call MULTIPLICAR;
  X := 25; Y := 3;  call DIVIDIR;
  X := 84; Y := 36; call MCD
end.
```

Para describir el lenguaje PL/0 se utilizó una alternativa a la notación BNF: los *grafos de sintaxis*. Ambas notaciones son equivalentes, aunque los grafos dan una imagen más clara de la estructura del lenguaje cuya sintaxis describen.

Hay un grafo de sintaxis por cada producción.

Los símbolos no terminales son representados mediante nombres encerrados en rectángulos, con excepción del símbolo inicial, que solamente aparece al comienzo de la primera producción.

Los símbolos terminales son representados mediante nombres encerrados en círculos o rectángulos con bordes redondeados, y pueden ser de dos tipos: si el nombre está en mayúsculas representa una palabra reservada del lenguaje, pero si está en minúsculas se trata del nombre de un grupo de símbolos terminales, y no de un símbolo propiamente dicho, ya que hacer una enumeración completa sería poco práctico (cuando no imposible).

A pesar de su pequeño tamaño, PL/0 es relativamente completo. La asignación es su proposición básica. Los conceptos fundamentales de la programación estructurada (secuencia, condición y repetición) están representados por las proposiciones *begin/end*, *if* y *while*. PL/0 incorpora el concepto de subrutina mediante declaraciones de procedimientos y proposiciones de llamadas a los mismos. Esto ofrece la oportunidad de presentar el concepto de localidad de las constantes, las variables y los procedimientos.

Para reducir su complejidad, PL/0 sólo ofrece un tipo de datos: los enteros (en este curso: enteros de 32 bits con signo). Es posible declarar variables y constantes de este tipo. PL/0 dispone de los operadores aritméticos y relacionales convencionales.

4. Análisis léxico

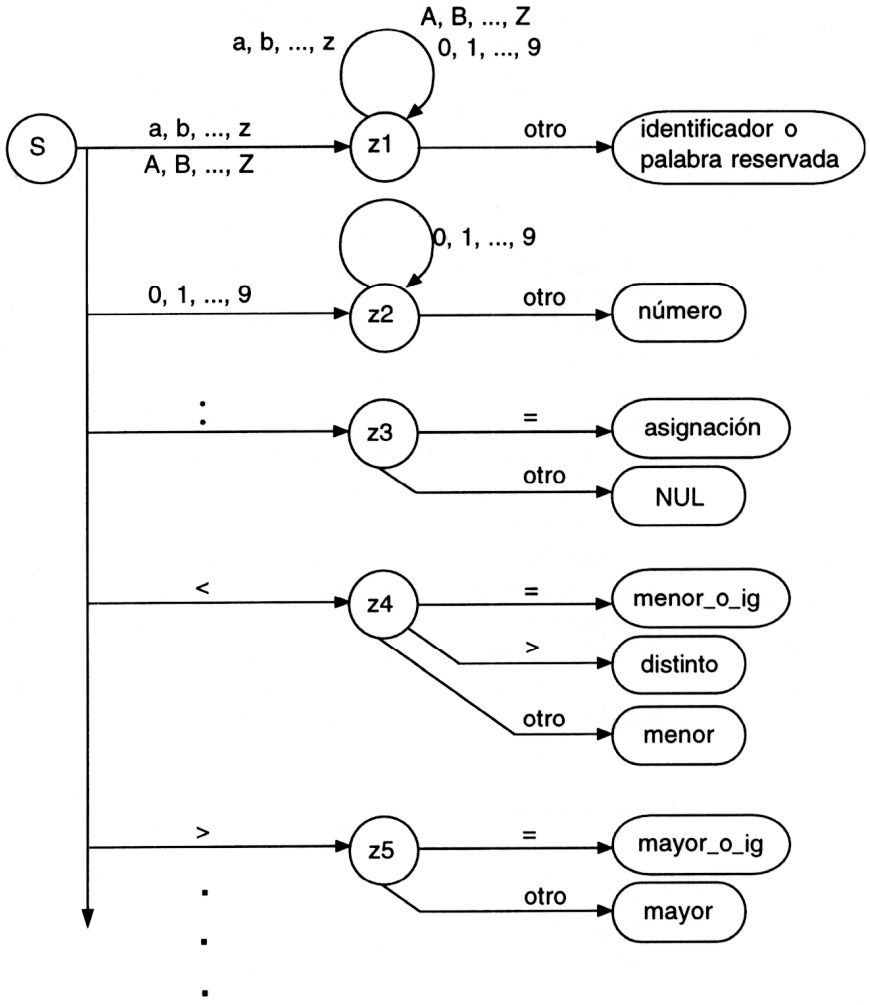
La tarea del analizador léxico consiste en:

a. **Saltear los separadores (blancos, tabulaciones, comentarios).**
b. **Reconocer los símbolos válidos e informar sobre los no válidos.**
c. **Llevar la cuenta de los renglones del programa.**
d. **Copiar los caracteres de entrada a la salida, generando un listado con los renglones numerados.**

El analizador léxico más simple es el de los lenguajes cuyos símbolos están compuestos por un único carácter. Esto no es lo más frecuente en el caso de los lenguajes de programación, donde las palabras reservadas, los identificadores, los números y los operadores pueden estar compuestos por más de un carácter. Para describir estos elementos, lo más conveniente es utilizar gramáticas regulares, o sea, gramáticas *G (T, N, P, S)* en las que cada producción *P* tiene la forma *A ::= aB* o *A ::= a*, y donde *A* y *B* pertenecen a *N* y *a* pertenece a *T*.

Es posible diseñar un autómata finito *F* para cada gramática regular *G*. Este autómata *F* acepta las frases del lenguaje definido por *G*, es decir, *L (G) = L (F)*.

A continuación, se presenta un diagrama de transición rudimentario del autómata que reconoce los símbolos del lenguaje PL/0.



El analizador léxico que se desarrollará para este curso deberá ser un procedimiento que tenga una forma similar a la siguiente (la forma, en definitiva, dependerá del lenguaje utilizado para implementarlo):

```
type terminal = (nulo, _begin, _call, _const, .... , coma, pto, ....);
     archivo = file of char;
     str63 = string [63];

procedure scanner (var Fuente, Listado: archivo; var S: terminal; var
Cad: str63; var Restante: string; var NumLinea: integer);
```

Cada vez que se llame al procedimiento scanner y la cadena Restante esté vacía o sólo contenga separadores, se leerá en Restante un nuevo renglón del archivo Fuente y se lo escribirá en el archivo Listado, anteponiéndole el valor actualizado de la variable NumLinea. Si, en cambio, la variable Restante contuviera caracteres útiles para formar símbolos, se los utilizará (borrándolos de Restante) para formar el próximo símbolo terminal S y la cadena de caracteres Cad correspondiente.

Por ejemplo, si el archivo Fuente contiene en sus dos primeros renglones:

```
CONST A=2;
procedure RAIZ;
```

Estos serán los valores luego de cada llamada:

Llamada	Listado	S	Cad	Restante	NumLinea
1	1: CONST A=2;	_const	'CONST'	' A=2;'	1
2	1: CONST A=2;	identificador	'A'	'=2;'	1
3	1: CONST A=2;	igual	'='	'2;'	1
4	1: CONST A=2;	numero	'2'	';'	1
5	1: CONST A=2;	ptoycoma	';'	''	1
6	1: CONST A=2; 2: procedure RAIZ;	_procedure	'PROCEDURE'	' RAIZ;'	2
7	1: CONST A=2; 2: procedure RAIZ;	identificador	'RAIZ'	';'	2
8	1: CONST A=2; 2: procedure RAIZ;	ptoycoma	';'	''	2

5. Análisis sintáctico

El proceso de determinar si una frase puede ser generada a partir de un conjunto de producciones se denomina *parsing*.

En el ejemplo 2, la frase *xyyz* se obtiene aplicando una vez *S* y tres veces *A* (las dos primeras veces que se aplica A se elige la opción de la derecha y la última vez la opción de la izquierda). Cuál producción se aplica surge inmediatamente al leer la frase de a un símbolo, de izquierda a derecha.

Veamos ahora el siguiente caso:

Ejemplo 3

S ::= A|B

A ::= xA|y

B ::= xB|z

Determinar las producciones aplicadas para generar *xxxxxxz* sólo es posible una vez que se leyó la frase completa, ya que habiendo leído sólo la primera *x* no es posible saber si al aplicar *S* corresponde elegir *A* o *B*.

Otro caso problemático se muestra a continuación:

Ejemplo 4

S ::= Ax

A ::= x|∈

Para generar la frase *x*, sólo es posible saber si corresponde aplicar la parte izquierda o la parte derecha de *A* una vez que *A* ya ha sido aplicada (bien o mal) y aparece la *x* final de *S*.

Las gramáticas que no presentan tales dificultades se denominan LL(1). La primera "L" significa que la entrada será leída de izquierda a derecha, y la segunda "L" indica derivaciones por la izquierda. El número "1" significa que alcanza con leer por anticipado un símbolo en cualquier paso del proceso de análisis sintáctico (o sea, solamente se emplea un símbolo de preanálisis). Al sistema de grafos con que se representa una gramática de este tipo se lo conoce como *grafo de sintaxis determinístico*.

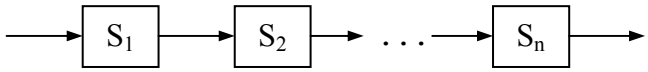
El paso siguiente consiste en construir un reconocedor sintáctico (*parser*) para una sintaxis dada. Este tipo de programa se deriva directamente del grafo de sintaxis determinístico y requiere de un procedimiento que funcione como scanner, salvo que los símbolos del lenguaje consten de un único carácter, en cuyo caso cualquier procedimiento de entrada estándar servirá para el ingreso del siguiente símbolo.

Para escribir un reconocedor sintáctico a partir de un grafo de sintaxis determinístico deberán seguirse las siguientes reglas:

R1. Reducir el sistema de grafos a la menor cantidad de grafos que sea posible, realizando para ello las sustituciones que sean necesarias.

R2. Declarar para cada grafo un procedimiento que contenga las sentencias resultantes de aplicarle al grafo las reglas R3 a R7.

R3. Una secuencia de elementos

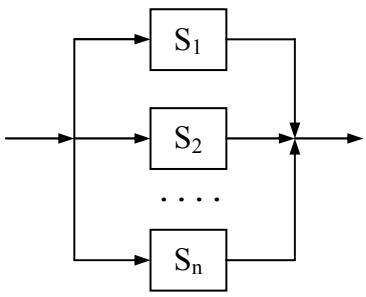


se traduce como una sentencia compuesta:

```
begin
  T(S1); T(S2); ... T(Sn)
end
```

(donde $T(S_i)$ es la sentencia obtenida al traducir el grafo S_i)

R4. Una opción entre elementos

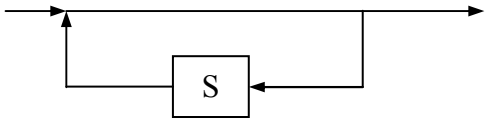


se traduce como una sentencia condicional:

if SIM in L_1 then T(S_1) else
if SIM in L_2 then T(S_2) else
....
if SIM in L_n then T(S_n);

donde SIM es el símbolo devuelto por el analizador léxico y L_i es el conjunto de símbolos iniciales de S_i. Siempre que L_i conste de un único símbolo *a*, "SIM in L_i" podrá expresarse como "SIM = *a*"

R5. Un bucle de la forma



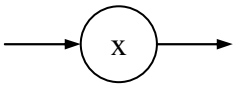
se traduce como la sentencia:

while SIM in L do T(S)

R6. Una referencia a otro grafo A

se traduce como una sentencia de llamada al procedimiento A

R7. Una referencia a un símbolo terminal x



se traduce como la sentencia:

if SIM = x then SCANNER(SIM) else ERROR

donde ERROR es un procedimiento encargado del tratamiento de los errores.

El parser funciona haciendo una llamada al scanner (para tener un símbolo leído de antemano) y una llamada al procedimiento correspondiente

al primero de los grafos. A partir de este procedimiento se irán realizando llamadas a los demás, hasta que aparezca algún error o se termine reconociendo satisfactoriamente el programa leído.

Algunas construcciones redundantes pueden suprimirse al depurar el parser resultante de la estricta aplicación de las reglas R1 a R7.

Veamos ahora el siguiente caso:

Ejemplo 5

A ::= x|(B)

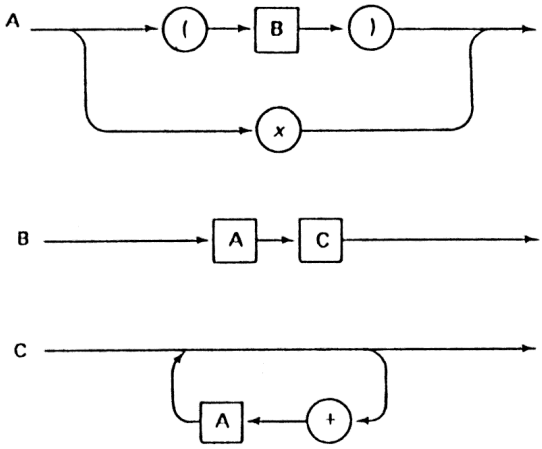
B ::= AC

C ::= {+A}

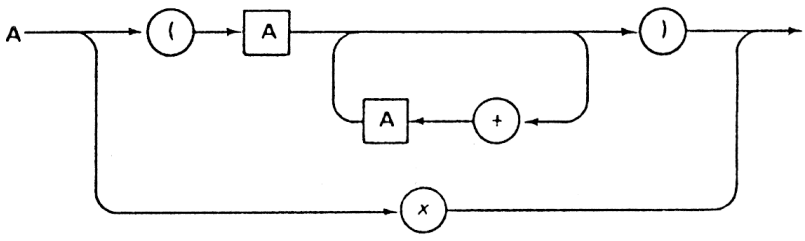
Aquí, los símbolos terminales son "x", "(", ")" y "+". Es posible utilizar el procedimiento *read* para llevar a cabo la función del scanner, ya que todos los símbolos están formados por un único carácter. Algunas de las posibles frases del lenguaje son:

x (x) (x+x) ((x))

Los grafos equivalentes a la gramática expresada en BNF son:



Aplicando la regla R1:



Aplicando las reglas R2 a R7:

```
program PARSER;
var SIM: char;
        procedure A;
        begin
          if SIM = 'x'
            then read (SIM)
            else if SIM = '('
                   then begin
                          read (SIM);
                          A;
                          while SIM = '+' do begin
                                              read (SIM);
                                              A
                                            end;
                          if SIM = ')' then read (SIM)
                                       else ERROR
                        end
                   else ERROR
        end;
begin
  read (SIM);
  A
end.
```

6. Análisis semántico

El análisis sintáctico no garantiza que un programa esté libre de errores. El siguiente programa escrito en PL/0 es sintácticamente correcto, pero contiene un error semántico, ya que un identificador de constante no puede ser llamado mediante la proposición call (que es exclusiva para identificadores de procedimiento).

Ejemplo 6

```
const K = 9;
var V;
procedure P;
  var X;
  begin
    X := K * 2;
    V := X
  end;
call K.
```

Para poder determinar si un programa es semánticamente correcto, el compilador deberá cargar en una tabla cada identificador que se declare. En esa tabla podrán consultarse:

- nombre del identificador
- tipo de identificador
- valor del identificador: Un número de 32 bits con distinto significado, según el tipo de identificador de que se trate:
  - ❒ constante: el valor de la constante
  - ❒ variable: la dirección de memoria a que se refiere la variable (sólo el desplazamiento)
  - ❒ procedimiento: la dirección de memoria donde comienza la proposición a ejecutar en el bloque

Una posible definición del tipo con que se declarará la tabla podría ser la siguiente:

```
type TABLA = array [0..MaxIdent-1] of record
                                        NOM: str63;
                                        TIPO: terminal;
                                        VALOR: longInt
                                     end;
```

El procedimiento BLOQUE recibirá como parámetro (pasaje por valor) la entrada de la tabla a partir de la cual se podrán cargar identificadores. Este parámetro podría llamarse BASE. Cuando se llama a BLOQUE desde el grafo PROGRAMA, se le pasa como parámetro el valor 0, ya que no hay identificadores previamente declarados.

El procedimiento BLOQUE contendrá un variable local llamada DESPLAZAMIENTO, que se irá incrementando con cada identificador que se declare. Cuando se llama a BLOQUE desde el grafo BLOQUE, se le pasa como parámetro el valor BASE+DESPLAZAMIENTO.

De esta forma, cada vez que se declare un identificador, deberá verificarse si éste ya había sido declarado en el mismo ámbito, es decir, entre las posiciones de la tabla delimitadas por BASE y BASE+DESPLAZAMIENTO-1.

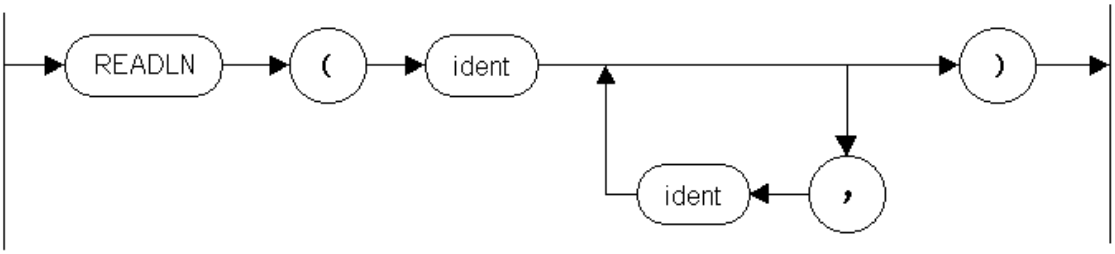
Para el análisis semántico, los identificadores se buscarán en toda la tabla, comenzando en la posición BASE+DESPLAZAMIENTO-1 y retrocediendo hasta la posición 0. De esta forma, siempre se encontrará primero el identificador que haya sido declarado localmente. En caso de no encontrarse el identificador, deberá darse aviso de la falta de declaración.

Una vez hallado el identificador en la tabla, con el campo TIPO podrá verificarse si el identificador es semánticamente correcto en la posición del programa donde fue encontrado.

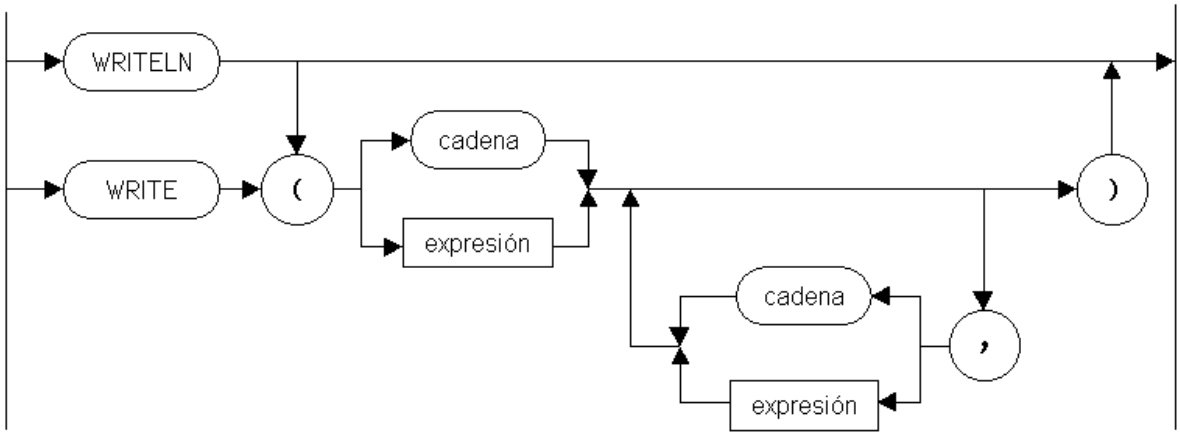
7. Generación de código

Antes de comenzar con el estudio de la generación de código, extenderemos la sintaxis de PL/0 mediante el agregado de tres proposiciones de E/S, ya que de lo contrario no podríamos ingresar valores en tiempo de ejecución ni podríamos ver los resultados de los cálculos realizados por el programa. Adoptaremos los nombres de los procedimientos de E/S de Pascal (*readln*, *write* y *writeln*), y les daremos una funcionalidad similar a la que tienen en este lenguaje cuando se los utiliza para realizar entrada desde el teclado y salida hacia la pantalla. Además, incorporaremos un símbolo terminal nuevo, la *cadena* literal, para permitir mostrar mensajes por pantalla. El analizador léxico considerará que cualquier secuencia de caracteres encerrada entre apóstrofos es una cadena.

La proposición de entrada READLN tendrá la sintaxis:



Las proposiciones de salida WRITELN y WRITE tendrán la sintaxis:



Finalmente, llegamos a la generación de código. Como plataforma de destino de la compilación, en este curso se adoptará una PC con un microprocesador que implemente IA-32 (Intel Architecture, 32-bit) y un sistema operativo compatible con la API Win32.

Utilizaremos (explícitamente) sólo 4 de los registros de 32 bits disponibles: EDI, EAX, EBX y EDX. Eventualmente, también accederemos a la parte baja de EAX, a través del subregistro AL (el cual permite acceder a los 8 bits menos significativos de EAX).

De los modos de direccionamiento soportados por el microprocesador, solamente vamos a usar los siguientes tres:

	EJEMPLOS	
modo registro	ADD EAX, EBX	(carga EAX con el valor de la suma de EAX más EBX)
modo inmediato	MOV EAX, 00000072	(carga EAX con el valor 00000072)
modo indexado	MOV EAX, [EDI+00000072]	(carga EAX con el contenido de la dirección EDI+00000072)

El archivo ejecutable generado por el compilador será de tipo PE (Portable Executable). Este tipo es compatible con las versiones de Windows actuales, ya que los ejecutables de tipo DOS COM (archivos COM), DOS MZ (archivos EXE) y NE (New Executable) corresponden a aplicaciones de 16 bits que no corren en las versiones de Windows de 64 bits.

El código del programa estará compuesto por una parte de longitud fija y una parte de longitud variable.

La parte de longitud fija contendrá:

- **un encabezado compatible con MS-DOS, caracterizado por el número mágico *4D 5A* (MZ), con instrucciones para avisar que la aplicación no es compatible con ese sistema operativo;**
- **los encabezados COFF (Common Object File Format), con su número mágico *50 45 00 00* (PE··) y OH (Optional Header), formados por numerosos campos usados para cargar y ejecutar la aplicación;**
- **una tabla de encabezados de secciones con el encabezado de *text*.**
- **el comienzo de la sección *text*, formado por instrucciones del x86 mediante las que se implementan las proposiciones de E/S. Estas instrucciones constituyen rutinas desde las cuales se realizarán las llamadas a las funciones de la API de Windows.**

La parte de longitud fija, inicialmente, deberá tener el siguiente contenido:

```
Offset      0  1  2  3  4  5  6  7   8  9  A  B  C  D  E  F

00000000   4D 5A 60 01 01 00 00 00  04 00 00 00 FF FF 00 00   MZ`.........ÿÿ..
00000010   60 01 00 00 00 00 00 00  40 00 00 00 00 00 00 00   `.......@.......
00000020   00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ................
00000030   00 00 00 00 00 00 00 00  00 00 00 00 A0 00 00 00   ............ ...
00000040   0E 1F BA 0E 00 B4 09 CD  21 B8 01 4C CD 21 54 68   ..º..´.Í!¸.LÍ!Th
00000050   69 73 20 70 72 6F 67 72  61 6D 20 69 73 20 61 20   is program is a
00000060   57 69 6E 33 32 20 63 6F  6E 73 6F 6C 65 20 61 70   Win32 console ap
00000070   70 6C 69 63 61 74 69 6F  6E 2E 20 49 74 20 63 61   plication. It ca
00000080   6E 6E 6F 74 20 62 65 20  72 75 6E 20 75 6E 64 65   nnot be run unde
00000090   72 20 4D 53 2D 44 4F 53  2E 0D 0A 24 00 00 00 00   r MS-DOS...$....
000000A0   50 45 00 00 4C 01 01 00  00 00 53 4C 00 00 00 00   PE..L.....SL....
000000B0   00 00 00 00 E0 00 02 01  0B 01 01 00 00 08 00 00   ....à...........
000000C0   00 00 00 00 00 00 00 00  00 15 00 00 00 10 00 00   ................
000000D0   00 20 00 00 00 00 40 00  00 10 00 00 00 02 00 00   . ....@.........
000000E0   04 00 00 00 00 00 00 00  04 00 00 00 00 00 00 00   ................
000000F0   00 20 00 00 00 02 00 00  00 00 00 00 03 00 00 00   . ..............
00000100   00 00 10 00 00 10 00 00  00 00 10 00 00 10 00 00   ................
00000110   00 00 00 00 10 00 00 00  00 00 00 00 00 00 00 00   ................
00000120   1C 10 00 00 28 00 00 00  00 00 00 00 00 00 00 00   ....(...........
00000130   00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ................
00000140   00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ................
00000150   00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ................
00000160   00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ................
00000170   00 00 00 00 00 00 00 00  00 10 00 00 1C 00 00 00   ................
00000180   00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ................
00000190   00 00 00 00 00 00 00 00  2E 74 65 78 74 00 00 00   .........text...
000001A0   0C 06 00 00 00 10 00 00  00 08 00 00 00 02 00 00   ................
000001B0   00 00 00 00 00 00 00 00  00 00 00 00 20 00 00 E0   ............ ..à
000001C0   00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ................
000001D0   00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ................
000001E0   00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ................
000001F0   00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ................
00000200   6E 10 00 00 7C 10 00 00  8C 10 00 00 98 10 00 00   n...|...Œ...˜...
00000210   A4 10 00 00 B6 10 00 00  00 00 00 00 52 10 00 00   ¤...¶.......R...
00000220   00 00 00 00 00 00 00 00  44 10 00 00 00 10 00 00   ........D.......
00000230   00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ................
00000240   00 00 00 00 4B 45 52 4E  45 4C 33 32 2E 64 6C 6C   ....KERNEL32.dll
00000250   00 00 6E 10 00 00 7C 10  00 00 8C 10 00 00 98 10   ..n...|...Œ...˜.
00000260   00 00 A4 10 00 00 B6 10  00 00 00 00 00 00 00 00   ..¤...¶.........
00000270   45 78 69 74 50 72 6F 63  65 73 73 00 00 00 47 65   ExitProcess...Ge
00000280   74 53 74 64 48 61 6E 64  6C 65 00 00 00 00 52 65   tStdHandle....Re
00000290   61 64 46 69 6C 65 00 00  00 00 57 72 69 74 65 46   adFile....WriteF
000002A0   69 6C 65 00 00 00 47 65  74 43 6F 6E 73 6F 6C 65   ile...GetConsole
000002B0   4D 6F 64 65 00 00 00 00  53 65 74 43 6F 6E 73 6F   Mode....SetConso
000002C0   6C 65 4D 6F 64 65 00 00  00 00 00 00 00 00 00 00   leMode..........
000002D0   50 A2 1C 11 40 00 31 C0  03 05 2C 11 40 00 75 0D   P¢..@.1À..,.@.u.
000002E0   6A F5 FF 15 04 10 40 00  A3 2C 11 40 00 6A 00 68   jõÿ...@.£,.@.j.h
000002F0   30 11 40 00 6A 01 68 1C  11 40 00 50 FF 15 0C 10   0.@.j.h..@.Pÿ...
00000300   40 00 09 C0 75 08 6A 00  FF 15 00 10 40 00 81 3D   @..Àu.j.ÿ...@.□=
00000310   30 11 40 00 01 00 00 00  75 EC 58 C3 00 57 72 69   0.@.....uìXÃ.Wri
00000320   74 65 20 65 72 72 6F 72  00 00 00 00 00 00 00 00   te error........
00000330   00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ................
00000340   60 31 C0 03 05 CC 11 40  00 75 37 6A F6 FF 15 04   `1À..Ì.@.u7jöÿ..
00000350   10 40 00 A3 CC 11 40 00  68 D0 11 40 00 50 FF 15   .@.£Ì.@.hÐ.@.Pÿ.
```

```
00000360   10 10 40 00 80 25 D0 11   40 00 F9 FF 35 D0 11 40   ..@.€%Ð.@.ùÿ5Ð.@
00000370   00 FF 35 CC 11 40 00 FF   15 14 10 40 00 A1 CC 11   .ÿ5Ì.@.ÿ...@.¡Ì.
00000380   40 00 6A 00 68 D4 11 40   00 6A 01 68 BE 11 40 00   @.j.hÔ.@.j.h¾.@.
00000390   50 FF 15 08 10 40 00 09   C0 61 90 75 08 6A 00 FF   Pÿ...@..Àa□u.j.ÿ
000003A0   15 00 10 40 00 0F B6 05   BE 11 40 00 81 3D D4 11   ...@..¶.¾.@.□=Ô.
000003B0   40 00 01 00 00 00 74 05   B8 FF FF FF FF C3 00 52   @.....t.¸ÿÿÿÿÃ.R
000003C0   65 61 64 20 65 72 72 6F   72 00 00 00 00 00 00 00   ead error.......
000003D0   00 00 00 00 00 00 00 00   00 00 00 00 00 00 00 00   ................
000003E0   60 89 C6 30 C0 02 06 74   08 46 E8 E1 FE FF FF EB   `‰Æ0À..t.Fèáþÿÿë
000003F0   F2 61 90 C3 00 00 00 00   00 00 00 00 00 00 00 00   òa□Ã............
00000400   04 30 E8 C9 FE FF FF C3   00 00 00 00 00 00 00 00   .0èÉþÿÿÃ........
00000410   B0 0D E8 B9 FE FF FF B0   0A E8 B2 FE FF FF C3 00   °.è¹þÿÿ°.è²þÿÿÃ.
00000420   3D 00 00 00 80 75 4E B0   2D E8 A2 FE FF FF B0 02   =...€uN°-è¢þÿÿ°.
00000430   E8 CB FF FF FF B0 01 E8   C4 FF FF FF B0 04 E8 BD   èËÿÿÿ°.èÄÿÿÿ°.è½
00000440   FF FF FF B0 07 E8 B6 FF   FF FF B0 04 E8 AF FF FF   ÿÿÿ°.è¶ÿÿÿ°.è¯ÿÿ
00000450   FF B0 08 E8 A8 FF FF FF   B0 03 E8 A1 FF FF FF B0   ÿ°.è¨ÿÿÿ°.è¡ÿÿÿ°
00000460   06 E8 9A FF FF FF B0 04   E8 93 FF FF FF B0 08 E8   .èšÿÿÿ°.è“ÿÿÿ°.è
00000470   8C FF FF FF C3 3D 00 00   00 00 7D 0B 50 B0 2D E8   Œÿÿÿà=....}.P°-è
00000480   4C FE FF FF 58 F7 D8 3D   0A 00 00 00 0F 8C EF 00   LþÿÿX÷Ø=.....Œï.
00000490   00 00 3D 64 00 00 00 0F   8C D1 00 00 00 3D E8 03   ..=d....ŒÑ...=è.
000004A0   00 00 0F 8C B3 00 00 00   3D 10 27 00 00 0F 8C 95   ...Œ³...=.'...Œ•
000004B0   00 00 00 3D A0 86 01 00   7C 7B 3D 40 42 0F 00 7C   ...= †..|{=@B..|
000004C0   61 3D 80 96 98 00 7C 47   3D 00 E1 F5 05 7C 2D 3D   a=€-˜.|G=.áõ.|-=
000004D0   00 CA 9A 3B 7C 13 BA 00   00 00 00 BB 00 CA 9A 3B   .Êš;|.º....».Êš;
000004E0   F7 FB 52 E8 18 FF FF FF   58 BA 00 00 00 00 BB 00   ÷ûRè.ÿÿÿXº....».
000004F0   E1 F5 05 F7 FB 52 E8 05   FF FF FF 58 BA 00 00 00   áõ.÷ûRè.ÿÿÿXº...
00000500   00 BB 80 96 98 00 F7 FB   52 E8 F2 FE FF FF 58 BA   .»€-˜.÷ûRèòþÿÿXº
00000510   00 00 00 00 BB 40 42 0F   00 F7 FB 52 E8 DF FE FF   ....»@B..÷ûRèßþÿ
00000520   FF 58 BA 00 00 00 00 BB   A0 86 01 00 F7 FB 52 E8   ÿXº....» †..÷ûRè
00000530   CC FE FF FF 58 BA 00 00   00 00 BB 10 27 00 00 F7   ÌþÿÿXº....».'..÷
00000540   FB 52 E8 B9 FE FF FF 58   BA 00 00 00 00 BB E8 03   ûRè¹þÿÿXº....»è.
00000550   00 00 F7 FB 52 E8 A6 FE   FF FF 58 BA 00 00 00 00   ..÷ûRè¦þÿÿXº....
00000560   BB 64 00 00 00 F7 FB 52   E8 93 FE FF FF 58 BA 00   »d...÷ûRè“þÿÿXº.
00000570   00 00 00 BB 0A 00 00 00   F7 FB 52 E8 80 FE FF FF   ...»....÷ûRè€þÿÿ
00000580   58 E8 7A FE FF FF C3 00   FF 15 00 10 40 00 00 00   Xèzþÿÿà.ÿ...@...
00000590   B9 00 00 00 00 B3 03 51   53 E8 A2 FD FF FF 5B 59   ¹....³.QSè¢ýÿÿ[Y
000005A0   3C 0D 0F 84 34 01 00 00   3C 08 0F 84 94 00 00 00   <..„4...<..„”...
000005B0   3C 2D 0F 84 09 01 00 00   3C 30 7C DB 3C 39 7F D7   <-.„....<0|Û<9□×
000005C0   2C 30 80 FB 00 74 D0 80   FB 02 75 0C 81 F9 00 00   ,0€û.tÐ€û.u.□ù..
000005D0   00 00 75 04 3C 00 74 BF   80 FB 03 75 0A 3C 00 75   ..u.<.t¿€û.u.<.u
000005E0   04 B3 00 EB 02 B3 01 81   F9 CC CC CC 0C 7F A8 81   .³.ë.³.□ùÌÌÌ.□¨□
000005F0   F9 34 33 33 F3 7C A0 88   C7 B8 0A 00 00 00 F7 E9   ù433ó| ˆÇ¸....÷é
00000600   3D 08 00 00 80 74 11 3D   F8 FF FF 7F 75 13 80 FF   =...€t.=øÿÿ□u.€ÿ
00000610   07 7E 0E E9 7F FF FF FF   80 FF 08 0F 8F 76 FF FF   .~.é□ÿÿÿ€ÿ..□vÿÿ
00000620   FF B9 00 00 00 00 88 F9   80 FB 02 74 04 01 C1 EB   ÿ¹....ˆù€û.t..Áë
00000630   03 29 C8 91 88 F8 51 53   E8 C3 FD FF FF 5B 59 E9   .)È‘ˆøQSèÃýÿÿ[Yé
00000640   53 FF FF FF 80 FB 03 0F   84 4A FF FF FF 51 53 B0   Sÿÿÿ€û..„Jÿÿÿ QS°
00000650   08 E8 7A FC FF FF B0 20   E8 73 FC FF FF B0 08 E8   .èzüÿÿ° èsüÿÿ°.è
00000660   6C FC FF FF 5B 59 80 FB   00 75 07 B3 03 E9 25 FF   lüÿÿ[Y€û.u.³.é%ÿ
00000670   FF FF 80 FB 02 75 0F 81   F9 00 00 00 00 75 07 B3   ÿÿ€û.u.□ù....u.³
00000680   03 E9 11 FF FF FF 89 C8   B9 0A 00 00 00 BA 00 00   .é.ÿÿÿ‰È¹....º..
00000690   00 00 3D 00 00 00 00 7D   08 F7 D8 F7 F9 F7 D8 EB   ..=....}.÷Ø÷ù÷Øë
000006A0   02 F7 F9 89 C1 81 F9 00   00 00 00 0F 85 E6 FE FF   .÷ù‰Á□ù.....…æþÿ
000006B0   FF 80 FB 02 0F 84 DD FE   FF FF B3 03 E9 D6 FE FF   ÿ€û..„Ýþÿÿ³.éÖþÿ
000006C0   FF 80 FB 03 0F 85 CD FE   FF FF B0 2D 51 53 E8 FD   ÿ€û..…Íþÿÿ°-QSèý
000006D0   FB FF FF 5B 59 B3 02 E9   BB FE FF FF 80 FB 03 0F   ûÿÿ[Y³.é»þÿÿ€û..
000006E0   84 B2 FE FF FF 80 FB 02   75 0C 81 F9 00 00 00 00   „²þÿÿ€û.u.□ù....
000006F0   0F 84 A1 FE FF FF 51 E8   14 FD FF FF 59 89 C8 C3   .„¡þÿÿQè.ýÿÿY‰ÈÃ
```

El significado de los campos de los encabezados es el siguiente:

```
/* MS-DOS COMPATIBLE HEADER */

memoria[0] = 0x4D; // 'M'  (Magic number)
memoria[1] = 0x5A; // 'Z'

memoria[2] = 0x60; // Bytes on last block
memoria[3] = 0x01; // (1 bl. = 512 bytes)

memoria[4] = 0x01; // Number of blocks
memoria[5] = 0x00; // in the EXE file

memoria[6] = 0x00; // Number of re-
memoria[7] = 0x00; // location entries

memoria[8] = 0x04; // Size of header
memoria[9] = 0x00; // (x 16 bytes)

memoria[10] = 0x00; // Minimum extra
memoria[11] = 0x00; // paragraphs needed

memoria[12] = 0xFF; // Maximum extra
memoria[13] = 0xFF; // paragraphs needed

memoria[14] = 0x00; // Initial (relative)
memoria[15] = 0x00; // SS value

memoria[16] = 0x60; // Initial SP value
memoria[17] = 0x01;

memoria[18] = 0x00; // Checksum
memoria[19] = 0x00;

memoria[20] = 0x00; // Initial IP value
memoria[21] = 0x00;

memoria[22] = 0x00; // Initial (relative)
memoria[23] = 0x00; // CS value

memoria[24] = 0x40; // Offset of the 1st
memoria[25] = 0x00; // relocation item

memoria[26] = 0x00; // Overlay number.
memoria[27] = 0x00; // (0 = main program)

memoria[28] = 0x00; // Reserved word
memoria[29] = 0x00;

memoria[30] = 0x00; // Reserved word
memoria[31] = 0x00;

memoria[32] = 0x00; // Reserved word
memoria[33] = 0x00;

memoria[34] = 0x00; // Reserved word
memoria[35] = 0x00;

memoria[36] = 0x00; // OEM identifier
memoria[37] = 0x00;

memoria[38] = 0x00; // OEM information
memoria[39] = 0x00;

memoria[40] = 0x00; // Reserved word
memoria[41] = 0x00;

memoria[42] = 0x00; // Reserved word
memoria[43] = 0x00;

memoria[44] = 0x00; // Reserved word
memoria[45] = 0x00;

memoria[46] = 0x00; // Reserved word
memoria[47] = 0x00;

memoria[48] = 0x00; // Reserved word
memoria[49] = 0x00;

memoria[50] = 0x00; // Reserved word
memoria[51] = 0x00;

memoria[52] = 0x00; // Reserved word
memoria[53] = 0x00;

memoria[54] = 0x00; // Reserved word
memoria[55] = 0x00;

memoria[56] = 0x00; // Reserved word
memoria[57] = 0x00;

memoria[58] = 0x00; // Reserved word
memoria[59] = 0x00;

memoria[60] = 0xA0; // Start of the COFF
memoria[61] = 0x00; // header
memoria[62] = 0x00;
memoria[63] = 0x00;

memoria[64] = 0x0E; // PUSH CS

memoria[65] = 0x1F; // POP DS

memoria[66] = 0xBA; // MOV DX,000E
memoria[67] = 0x0E;
memoria[68] = 0x00;

memoria[69] = 0xB4; // MOV AH,09
memoria[70] = 0x09;

memoria[71] = 0xCD; // INT 21
memoria[72] = 0x21;

memoria[73] = 0xB8; // MOV AX,4C01
memoria[74] = 0x01;
memoria[75] = 0x4C;

memoria[76] = 0xCD; // INT 21
memoria[77] = 0x21;

memoria[78] = 0x54; // 'T'
memoria[79] = 0x68; // 'h'
memoria[80] = 0x69; // 'i'
memoria[81] = 0x73; // 's'
memoria[82] = 0x20; // ' '
memoria[83] = 0x70; // 'p'
memoria[84] = 0x72; // 'r'
memoria[85] = 0x6F; // 'o'
memoria[86] = 0x67; // 'g'
memoria[87] = 0x72; // 'r'
memoria[88] = 0x61; // 'a'
```

```
memoria[89] = 0x6D; // 'm'
memoria[90] = 0x20; // ' '
memoria[91] = 0x69; // 'i'
memoria[92] = 0x73; // 's'
memoria[93] = 0x20; // ' '
memoria[94] = 0x61; // 'a'
memoria[95] = 0x20; // ' '
memoria[96] = 0x57; // 'W'
memoria[97] = 0x69; // 'i'
memoria[98] = 0x6E; // 'n'
memoria[99] = 0x33; // '3'
memoria[100] = 0x32; // '2'
memoria[101] = 0x20; // ' '
memoria[102] = 0x63; // 'c'
memoria[103] = 0x6F; // 'o'
memoria[104] = 0x6E; // 'n'
memoria[105] = 0x73; // 's'
memoria[106] = 0x6F; // 'o'
memoria[107] = 0x6C; // 'l'
memoria[108] = 0x65; // 'e'
memoria[109] = 0x20; // ' '
memoria[110] = 0x61; // 'a'
memoria[111] = 0x70; // 'p'
memoria[112] = 0x70; // 'p'
memoria[113] = 0x6C; // 'l'
memoria[114] = 0x69; // 'i'
memoria[115] = 0x63; // 'c'
memoria[116] = 0x61; // 'a'
memoria[117] = 0x74; // 't'
memoria[118] = 0x69; // 'i'
memoria[119] = 0x6F; // 'o'
memoria[120] = 0x6E; // 'n'
memoria[121] = 0x2E; // '.'
memoria[122] = 0x20; // ' '
memoria[123] = 0x49; // 'I'
memoria[124] = 0x74; // 't'
memoria[125] = 0x20; // ' '
memoria[126] = 0x63; // 'c'
memoria[127] = 0x61; // 'a'
memoria[128] = 0x6E; // 'n'
memoria[129] = 0x6E; // 'n'
memoria[130] = 0x6F; // 'o'
memoria[131] = 0x74; // 't'
memoria[132] = 0x20; // ' '
memoria[133] = 0x62; // 'b'
memoria[134] = 0x65; // 'e'
memoria[135] = 0x20; // ' '
memoria[136] = 0x72; // 'r'
memoria[137] = 0x75; // 'u'
memoria[138] = 0x6E; // 'n'
memoria[139] = 0x20; // ' '
memoria[140] = 0x75; // 'u'
memoria[141] = 0x6E; // 'n'
memoria[142] = 0x64; // 'd'
memoria[143] = 0x65; // 'e'
memoria[144] = 0x72; // 'r'
memoria[145] = 0x20; // ' '
memoria[146] = 0x4D; // 'M'
memoria[147] = 0x53; // 'S'
memoria[148] = 0x2D; // '-'
memoria[149] = 0x44; // 'D'
memoria[150] = 0x4F; // 'O'
memoria[151] = 0x53; // 'S'
memoria[152] = 0x2E; // '.'
memoria[153] = 0x0D; // Carriage return
memoria[154] = 0x0A; // Line feed
memoria[155] = 0x24; // String end ('$')
memoria[156] = 0x00;
memoria[157] = 0x00;
memoria[158] = 0x00;
memoria[159] = 0x00;

/* COFF HEADER - 8 Standard fields */

memoria[160] = 0x50; // 'P'
memoria[161] = 0x45; // 'E'
memoria[162] = 0x00; // '\0'
memoria[163] = 0x00; // '\0'

memoria[164] = 0x4C; // Machine:
memoria[165] = 0x01; // >= Intel 386

memoria[166] = 0x01; // Number of
memoria[167] = 0x00; // sections

memoria[168] = 0x00; // Time/Date stamp
memoria[169] = 0x00;
memoria[170] = 0x53;
memoria[171] = 0x4C;

memoria[172] = 0x00; // Pointer to symbol
memoria[173] = 0x00; // table
memoria[174] = 0x00; // (deprecated)
memoria[175] = 0x00;

memoria[176] = 0x00; // Number of symbols
memoria[177] = 0x00; // (deprecated)
memoria[178] = 0x00;
memoria[179] = 0x00;

memoria[180] = 0xE0; // Size of optional
memoria[181] = 0x00; // header

memoria[182] = 0x02; // Characteristics:
memoria[183] = 0x01; // 32BIT_MACHINE EXE

/* OPTIONAL HEADER - 8 Standard fields */
/*  (For image files, it is required)  */

memoria[184] = 0x0B; // Magic number
memoria[185] = 0x01; // (010B = PE32)

memoria[186] = 0x01;// Maj.Linker Version

memoria[187] = 0x00;// Min.Linker Version

memoria[188] = 0x00; // Size of code
memoria[189] = 0x06; // (text) section
memoria[190] = 0x00;
memoria[191] = 0x00;

memoria[192] = 0x00; // Size of
memoria[193] = 0x00; // initialized data
memoria[194] = 0x00; // section
memoria[195] = 0x00;

memoria[196] = 0x00; // Size of
memoria[197] = 0x00; // uninitialized
memoria[198] = 0x00; // data section
memoria[199] = 0x00;
```

```
memoria[200] = 0x00; // Starting address
memoria[201] = 0x15; // relative to the
memoria[202] = 0x00; // image base
memoria[203] = 0x00;

memoria[204] = 0x00; // Base of code
memoria[205] = 0x10;
memoria[206] = 0x00;
memoria[207] = 0x00;

/* OPT.HEADER - 1 PE32 specific field */

memoria[208] = 0x00; // Base of data
memoria[209] = 0x20;
memoria[210] = 0x00;
memoria[211] = 0x00;

/* OPT.HEADER - 21 Win-Specific Fields */

memoria[212] = 0x00; // Image base
memoria[213] = 0x00; // (Preferred
memoria[214] = 0x40; // address of image
memoria[215] = 0x00; // when loaded)

memoria[216] = 0x00; // Section alignment
memoria[217] = 0x10;
memoria[218] = 0x00;
memoria[219] = 0x00;

memoria[220] = 0x00; // File alignment
memoria[221] = 0x02; // (Default is 512)
memoria[222] = 0x00;
memoria[223] = 0x00;

memoria[224] = 0x04; // Major OS version
memoria[225] = 0x00;

memoria[226] = 0x00; // Minor OS version
memoria[227] = 0x00;

memoria[228] = 0x00;// Maj. image version
memoria[229] = 0x00;

memoria[230] = 0x00;// Min. image version
memoria[231] = 0x00;

memoria[232] = 0x04;// Maj.subsystem ver.
memoria[233] = 0x00;

memoria[234] = 0x00;// Min.subsystem ver.
memoria[235] = 0x00;

memoria[236] = 0x00; // Win32 version
memoria[237] = 0x00; // (Reserved, must
memoria[238] = 0x00; // be zero)
memoria[239] = 0x00;

memoria[240] = 0x00;// Size of image
memoria[241] = 0x20;// (It must be a
memoria[242] = 0x00;// multiple of the
memoria[243] = 0x00;// section alignment)

memoria[244] = 0x00; // Size of headers
memoria[245] = 0x02; // (rounded up to a
memoria[246] = 0x00; // multiple of the
memoria[247] = 0x00; // file alignment)

memoria[248] = 0x00; // Checksum
memoria[249] = 0x00;
memoria[250] = 0x00;
memoria[251] = 0x00;

memoria[252] = 0x03; // Windows subsystem
memoria[253] = 0x00; // (03 = console)

memoria[254] = 0x00; // DLL charac-
memoria[255] = 0x00; // teristics

memoria[256] = 0x00; // Size of stack
memoria[257] = 0x00; // reserve
memoria[258] = 0x10;
memoria[259] = 0x00;

memoria[260] = 0x00; // Size of stack
memoria[261] = 0x10; // commit
memoria[262] = 0x00;
memoria[263] = 0x00;

memoria[264] = 0x00; // Size of heap
memoria[265] = 0x00; // reserve
memoria[266] = 0x10;
memoria[267] = 0x00;

memoria[268] = 0x00; // Size of heap
memoria[269] = 0x10; // commit
memoria[270] = 0x00;
memoria[271] = 0x00;

memoria[272] = 0x00; // Loader flags
memoria[273] = 0x00; // (Reserved, must
memoria[274] = 0x00; // be zero)
memoria[275] = 0x00;

memoria[276] = 0x10; // Number of
memoria[277] = 0x00; // relative virtual
memoria[278] = 0x00; // addresses (RVAs)
memoria[279] = 0x00;

/* OPT. HEADER - 16 Data Directories */

memoria[280] = 0x00; // Export Table
memoria[281] = 0x00;
memoria[282] = 0x00;
memoria[283] = 0x00;
memoria[284] = 0x00;
memoria[285] = 0x00;
memoria[286] = 0x00;
memoria[287] = 0x00;

memoria[288] = 0x1C; // Import Table
memoria[289] = 0x10;
memoria[290] = 0x00;
memoria[291] = 0x00;
memoria[292] = 0x28;
memoria[293] = 0x00;
memoria[294] = 0x00;
memoria[295] = 0x00;

memoria[296] = 0x00; // Resource Table
memoria[297] = 0x00;
memoria[298] = 0x00;
memoria[299] = 0x00;
memoria[300] = 0x00;
```

```
memoria[301] = 0x00;
memoria[302] = 0x00;
memoria[303] = 0x00;

memoria[304] = 0x00; // Exception Table
memoria[305] = 0x00;
memoria[306] = 0x00;
memoria[307] = 0x00;
memoria[308] = 0x00;
memoria[309] = 0x00;
memoria[310] = 0x00;
memoria[311] = 0x00;

memoria[312] = 0x00; // Certificate Table
memoria[313] = 0x00;
memoria[314] = 0x00;
memoria[315] = 0x00;
memoria[316] = 0x00;
memoria[317] = 0x00;
memoria[318] = 0x00;
memoria[319] = 0x00;

memoria[320] = 0x00; // Base Relocation
memoria[321] = 0x00; // Table
memoria[322] = 0x00;
memoria[323] = 0x00;
memoria[324] = 0x00;
memoria[325] = 0x00;
memoria[326] = 0x00;
memoria[327] = 0x00;

memoria[328] = 0x00; // Debug
memoria[329] = 0x00;
memoria[330] = 0x00;
memoria[331] = 0x00;
memoria[332] = 0x00;
memoria[333] = 0x00;
memoria[334] = 0x00;
memoria[335] = 0x00;

memoria[336] = 0x00; // Architecture
memoria[337] = 0x00;
memoria[338] = 0x00;
memoria[339] = 0x00;
memoria[340] = 0x00;
memoria[341] = 0x00;
memoria[342] = 0x00;
memoria[343] = 0x00;

memoria[344] = 0x00; // Global Ptr
memoria[345] = 0x00;
memoria[346] = 0x00;
memoria[347] = 0x00;
memoria[348] = 0x00;
memoria[349] = 0x00;
memoria[350] = 0x00;
memoria[351] = 0x00;

memoria[352] = 0x00; // TLS Table
memoria[353] = 0x00;
memoria[354] = 0x00;
memoria[355] = 0x00;
memoria[356] = 0x00;
memoria[357] = 0x00;
memoria[358] = 0x00;
memoria[359] = 0x00;

memoria[360] = 0x00; // Load Config Table
memoria[361] = 0x00;
memoria[362] = 0x00;
memoria[363] = 0x00;
memoria[364] = 0x00;
memoria[365] = 0x00;
memoria[366] = 0x00;
memoria[367] = 0x00;

memoria[368] = 0x00; // Bound Import
memoria[369] = 0x00;
memoria[370] = 0x00;
memoria[371] = 0x00;
memoria[372] = 0x00;
memoria[373] = 0x00;
memoria[374] = 0x00;
memoria[375] = 0x00;

memoria[376] = 0x00; // IAT
memoria[377] = 0x10;
memoria[378] = 0x00;
memoria[379] = 0x00;
memoria[380] = 0x1C;
memoria[381] = 0x00;
memoria[382] = 0x00;
memoria[383] = 0x00;

memoria[384] = 0x00; // Delay Import
memoria[385] = 0x00; // Descriptor
memoria[386] = 0x00;
memoria[387] = 0x00;
memoria[388] = 0x00;
memoria[389] = 0x00;
memoria[390] = 0x00;
memoria[391] = 0x00;

memoria[392] = 0x00; // CLR Runtime
memoria[393] = 0x00; // Header
memoria[394] = 0x00;
memoria[395] = 0x00;
memoria[396] = 0x00;
memoria[397] = 0x00;
memoria[398] = 0x00;
memoria[399] = 0x00;

memoria[400] = 0x00; // Reserved, must be
memoria[401] = 0x00; // zero
memoria[402] = 0x00;
memoria[403] = 0x00;
memoria[404] = 0x00;
memoria[405] = 0x00;
memoria[406] = 0x00;
memoria[407] = 0x00;

/* SECTIONS TABLE (40 bytes per entry) */

/* FIRST ENTRY: TEXT HEADER */

memoria[408] = 0x2E; // '.' (Name)
memoria[409] = 0x74; // 't'
memoria[410] = 0x65; // 'e'
memoria[411] = 0x78; // 'x'
memoria[412] = 0x74; // 't'
memoria[413] = 0x00;
memoria[414] = 0x00;
memoria[415] = 0x00;
```

```
memoria[416] = 0x24; // Virtual size
memoria[417] = 0x05;
memoria[418] = 0x00;
memoria[419] = 0x00;

memoria[420] = 0x00; // Virtual address
memoria[421] = 0x10;
memoria[422] = 0x00;
memoria[423] = 0x00;

memoria[424] = 0x00; // Size of raw data
memoria[425] = 0x06;
memoria[426] = 0x00;
memoria[427] = 0x00;

memoria[428] = 0x00; // Pointer to
memoria[429] = 0x02; // raw data
memoria[430] = 0x00;
memoria[431] = 0x00;

memoria[432] = 0x00; // Pointer to
memoria[433] = 0x00; // relocations
memoria[434] = 0x00;
memoria[435] = 0x00;

memoria[436] = 0x00; // Pointer to
memoria[437] = 0x00; // line numbers
memoria[438] = 0x00;
memoria[439] = 0x00;

memoria[440] = 0x00; // Number of
memoria[441] = 0x00; // relocations

memoria[442] = 0x00; // Number of
memoria[443] = 0x00; // line numbers

memoria[444] = 0x20; // Characteristics
memoria[445] = 0x00; // (Readable,
memoria[446] = 0x00; // Writeable &
memoria[447] = 0xE0; // Executable)
```

Las posiciones 428-431 (01AC-01AF en hexadecimal) contienen la dirección de inicio de la sección *text*, que es donde estará ubicado el código ejecutable (las rutinas de E/S y la traducción del programa escrito en PL/0). Por lo tanto, las posiciones 448-511 (01C0-01FF en hexadecimal) deberán rellenarse con ceros, para que la sección *text* comience en la posición 512 (0200 en hexadecimal).

La parte de longitud fija de la sección *text* contiene el código de las rutinas de E/S, de 512 a 1791 (0200-06FF en hexadecimal). Para poder invocar estas rutinas, no es necesario conocer su funcionamiento interno, ya que alcanza con saber en qué posición comienza cada una:

- **992 (03E0 en hexadecimal): muestra por consola una cadena terminada en cero, alojada a partir de la dirección guardada en EAX.**
- **1040 (0410 en hexadecimal): envía un salto de línea a la consola.**
- **1056 (0420 en hexadecimal): muestra por consola el número entero contenido en EAX.**
- **1416 (0588 en hexadecimal): finaliza el programa**
- **1424 (0590 en hexadecimal): lee por consola un número entero y lo deja guardado en EAX.**

La parte de longitud variable de la sección *text* contendrá las instrucciones resultantes de traducir el programa fuente escrito en PL/0. La traducción consiste en escribir instrucciones, byte a byte, en el archivo ejecutable. Estos bytes corresponderán a las siguientes instrucciones del x86 (los valores están en hexadecimal):

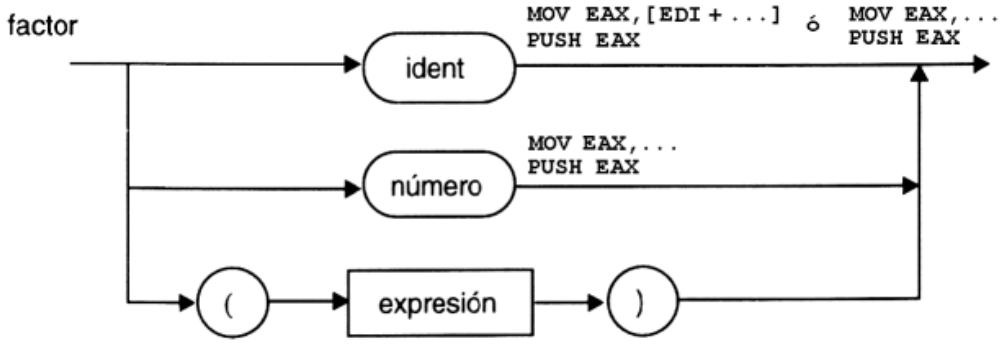
MNEMÓNICO	BYTES	SIGNIFICADO
MOV EDI, *abcdefgh*	BF *gh ef cd ab*	COPIA EL SEGUNDO OPERANDO EN EL PRIMERO
MOV EAX, [EDI+*abcdefgh*]	8B 87 *gh ef cd ab*	
MOV [EDI+*abcdefgh*], EAX	89 87 *gh ef cd ab*	
MOV EAX, *abcdefgh*	B8 *gh ef cd ab*	
XCHG EAX, EBX	93	INTERCAMBIA LOS VALORES DE LOS OPERANDOS
PUSH EAX	50	MANDA EL VALOR DEL OPERANDO A LA PILA
POP EAX	58	EXTRAE EL VALOR DE LA PILA Y LO COLOCA EN EL OPERANDO
POP EBX	5B	
ADD EAX, EBX	01 D8	SUMA AMBOS OPERANDOS Y COLOCA EL RESULTADO EN EL PRIMERO
SUB EAX, EBX	29 D8	LE RESTA EL SEGUNDO OPERANDO AL PRIMERO Y COLOCA EL RESULTADO EN EL PRIMER OPERANDO
IMUL EBX	F7 EB	COLOCA EN EDX:EAX EL PRODUCTO DE EAX POR EBX
IDIV EBX	F7 FB	DIVIDE EDX:EAX POR EL OPERANDO Y COLOCA EL COCIENTE EN EAX Y EL RESTO EN EDX
CDQ	99	LLENA TODOS LOS BITS DE EDX CON EL VALOR DEL BIT DEL SIGNO DE EAX
NEG EAX	F7 D8	CAMBIA EL SIGNO DE EAX
TEST AL, *ab*	A8 *ab*	CALCULA EL "Y" ENTRE LOS OPERANDOS Y MODIFICA VARIAS BANDERAS, ENTRE ELLAS PF (PARITY FLAG)
CMP EBX, EAX	39 C3	COMPARA EL PRIMER OPERANDO CON EL SEGUNDO PARA QUE, SEGÚN EL RESULTADO DE LA COMPARACIÓN, PUEDAN HACERSE SALTOS CONDICIONALES A CONTINUACIÓN
JE *dir* JZ *dir*	74 *ab*	SEGÚN EL RESULTADO DE UNA COMPARACIÓN, SALTA A LA DIRECCIÓN UBICADA *ab* BYTES ANTES O DESPUÉS DE LA DIRECCIÓN ACTUAL. JE (JUMP IF =) JNE (JUMP IF NOT =) JG (JUMP IF >) JGE (JUMP IF > OR =) JL (JUMP IF <) JLE (JUMP IF < OR =) JPO (JUMP IF PARITY ODD)
JNE *dir* JNZ *dir*	75 *ab*	
JG *dir*	7F *ab*	
JGE *dir*	7D *ab*	
JL *dir*	7C *ab*	
JLE *dir*	7E *ab*	
JPO *dir*	7B *ab*	
JMP *dir*	E9 *gh ef cd ab*	SALTA A LA DIRECCIÓN UBICADA *abcdefgh* BYTES ANTES O DESPUÉS DE LA DIRECCIÓN ACTUAL
CALL *dir*	E8 *gh ef cd ab*	INVOCA LA SUBRUTINA UBICADA *abcdefgh* BYTES ANTES O DESPUÉS DE LA DIRECCIÓN ACTUAL
RET	C3	RETORNA AL PUNTO DESDE DONDE SE LLAMÓ UNA SUBRUTINA

Los valores *ab* y *abcdefgh* representan números enteros de 8 y 32 bits, respectivamente. En las instrucciones, *abcdefgh* aparece invertido.

La primera instrucción del código traducido será la inicialización del registro EDI para que apunte a la dirección a partir de la cual estarán alojados los valores de las variables. Como esta dirección aún no se conoce, deberá reservarse el lugar grabando `BF 00 00 00 00`.

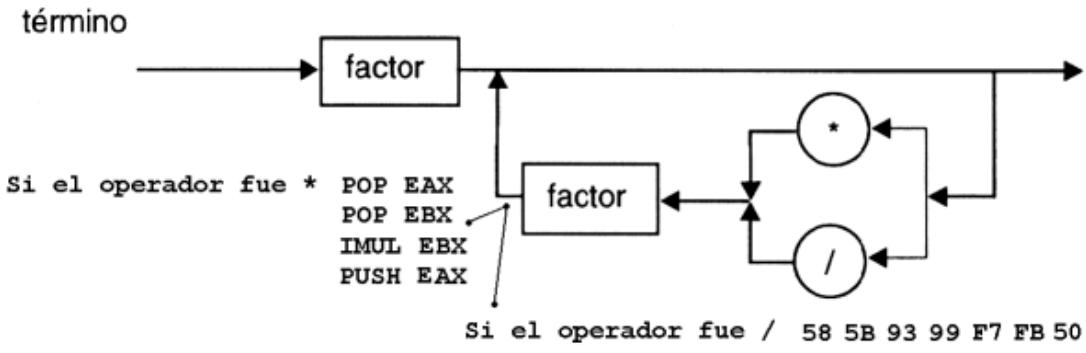
Un programa escrito en PL/0 hará uso intensivo de la pila. La idea general es que los factores se colocarán en la pila (con PUSH) para ser retirados (con POP) siempre que haya que calcular el valor de un término, una expresión o una condición.

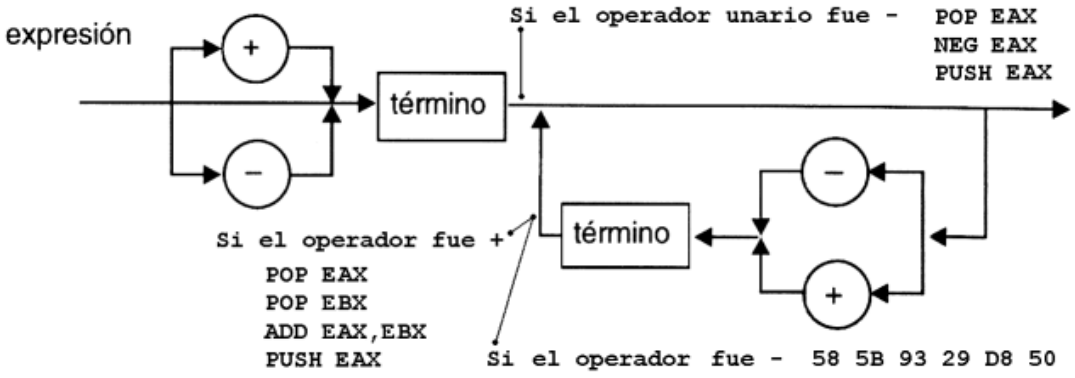
Para ver en detalle qué instrucciones deberán generarse (es decir, qué bytes deberán escribirse en la sección *text* del archivo ejecutable), se analizarán detenidamente los grafos de sintaxis de PL/0 ya vistos en la pág. 6. Comencemos por *factor*:



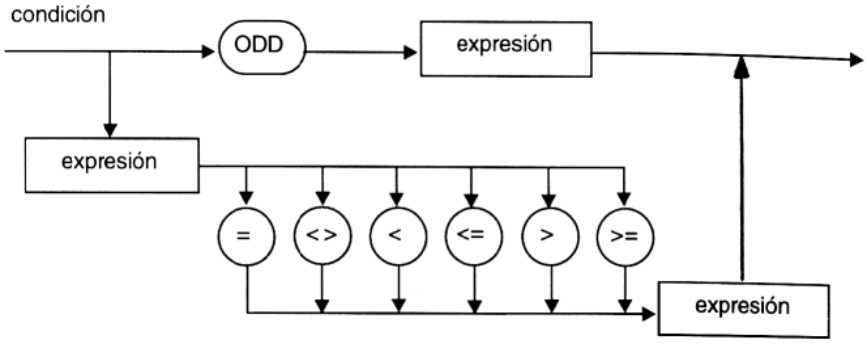
La instrucción MOV debe completarse con los cuatro bytes correspondientes a un valor numérico (si el identificador se refiere a una constante o si en el código fuente aparece directamente un número) o a un desplazamiento en memoria relativo al valor contenido en EDI (si el identificador se refiere a una variable). Como son dos instrucciones diferentes, deben usarse bytes diferentes (B8 y 8B 87, respectivamente).

En *término* y *expresión*, deben grabarse las siguientes instrucciones:





En *condición* deben generarse instrucciones para que, según una expresión (la que aparece luego de ODD) o dos expresiones (las que están relacionadas mediante los operadores lógicos) se ejecuten o se salteen las instrucciones generadas por la *proposición* que siempre viene a continuación (*condición* solamente es llamado desde *if* y desde *while*).



Los bytes generados luego de la *expresión* que sucede a ODD son: 58 A8 01 7B 05 E9 00 00 00 00.

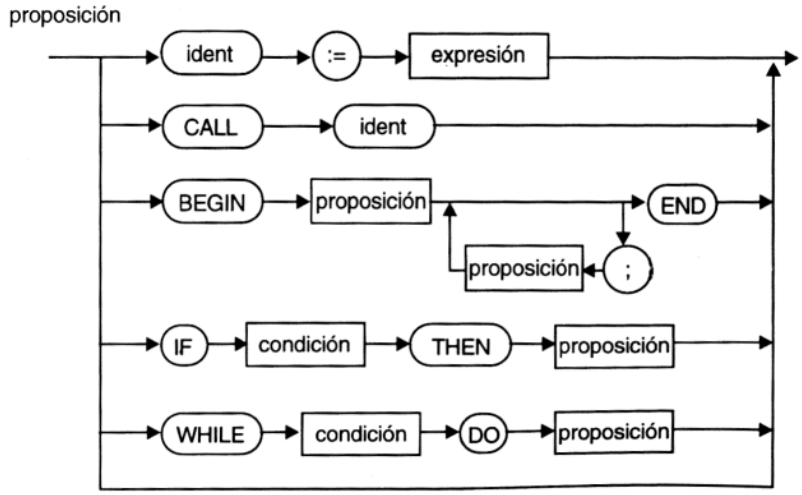
Las instrucciones generadas luego de la segunda *expresión* en la parte inferior del grafo son todas iguales, salvo por un salto condicional (de 2 bytes) que es específico del operador booleano:
58 5B 39 C3

=	<>	<	<=	>	>=
74 05	75 05	7C 05	7E 05	7F 05	7D 05

E9 00 00 00 00

Como no se conoce de antemano la cantidad de bytes que deben saltearse, se genera un salto E9 00 00 00 00 "para reservar el lugar". Luego de generar las instrucciones de la *proposición*, se debe volver atrás para corregir el destino del salto. Esto se conoce como "fix-up".

Veamos ahora los distintos casos de *proposición*:



En la asignación (y también en *READLN*), el valor del registro EAX (traído con POP EAX de la pila donde fue depositado por *expresión* o ingresado desde el teclado mediante una invocación a la rutina de entrada de enteros usando una instrucción CALL) debe copiarse a la posición de memoria correspondiente a la variable representada por el identificador.

En *CALL* debe generarse una instrucción homónima basada en la dirección de memoria del procedimiento que está siendo llamado, por ejemplo: E8 56 FF FF FF. Cabe aclarar que FFFFFF56 indica la cantidad de bytes a saltar (aquí se trata de un salto hacia atrás, por ser FFFFFF56 un número negativo), no la dirección absoluta del procedimiento.

La proposición *IF* no genera instrucciones, simplemente realiza el fix-up del salto generado por *condición*.

La proposición *WHILE* coloca un salto hacia arriba (para volver a evaluar la condición) inmediatamente a continuación de las instrucciones generadas por *proposición*, para luego realizar el fix-up del salto generado por *condición*.

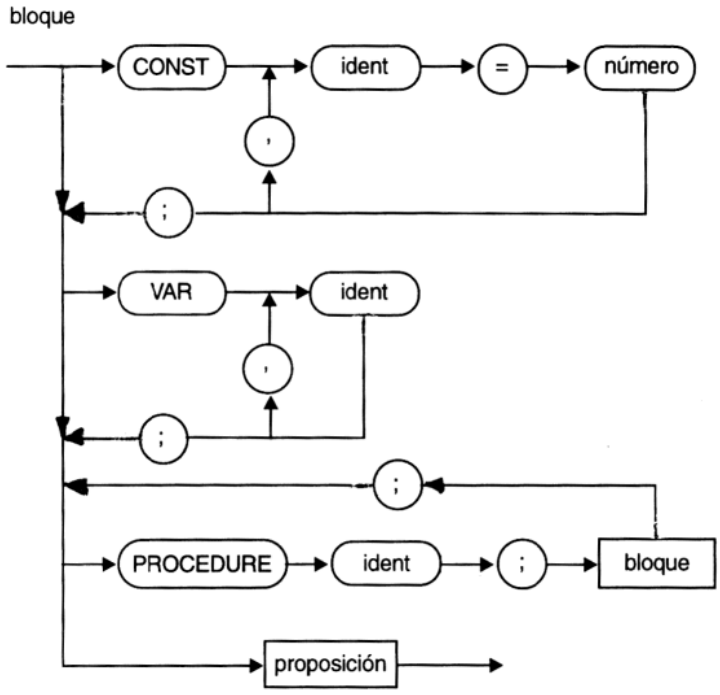
La proposiciones *WRITE* y *WRITELN* se comportan de dos formas diferentes, según se utilicen para imprimir resultados de expresiones o cadenas.

Los resultados de las expresiones se sacan de la pila (con POP EAX) y se muestran llamando a la rutina de salida de números (con CALL).

La generación del código para imprimir cadenas consta de los siguientes pasos:

1. **Se genera la inicialización de EAX con la ubicación absoluta que tendrá la cadena (se conoce porque la longitud de los pasos 2 y 3 es fija), usando para calcularla los campos *BaseOfCode* (posiciones 204-207, o 00CC-00CF en hexadecimal) e *ImageBase* (posiciones 212-215, o 00D4-00D7 en hexadecimal) del encabezado del archivo ejecutable;**
2. **Se genera la invocación a la rutina de E/S que mostrará la cadena;**
3. **Se genera un salto incondicional E9 00 00 00 00;**
4. **Se generan los bytes de la cadena, seguidos de un cero;**
5. **Se realiza el fix-up del salto colocado en el paso 3.**

Veamos ahora la generación del código en *bloque*:



Al ingresar a *bloque* debe insertarse un salto, que dirige la ejecución hacia la primera instrucción de la primera proposición del bloque, salteando las instrucciones generadas al traducir los procedimientos locales que pudiera haber. El fix-up de este salto debe hacerse justo antes de entrar a *proposición*.

Al salir de *bloque* en *PROCEDURE* debe generarse una instrucción RET (código C3).

La salida del programa se lleva a cabo generando un salto (no una invocación) hacia la rutina de E/S que finaliza el programa.

En este momento de la compilación, el análisis del código fuente ya finalizó, y no quedan instrucciones por grabar.

A continuación, se debe hacer un *fix-up* de la primera instrucción de la parte de longitud variable de la sección *text* (MOV EDI, 00000000), ya que el desplazamiento actual en el archivo ejecutable indica el comienzo del área de almacenamiento de las variables.

Luego, deben grabarse ceros al final del archivo ejecutable, a razón de cuatro bytes por cada variable (a esta altura de la compilación, el número de variables que fueron declaradas ya es conocido).

Ahora se debe realizar el ajuste del campo *VirtualSize* del encabezado de la sección *text* (posiciones 416-419, o 01A0-01A3 en hexadecimal), colocando allí el tamaño de la sección *text* (hasta el momento).

Después, debe rellenarse el archivo con ceros, para que su tamaño sea múltiplo del campo *FileAlignment* del encabezado opcional específico para Windows (posiciones 220-223, o 00DC-00DF en hexadecimal).

En este momento, es necesario ajustar los campos *SizeOfCodeSection* (posiciones 188-191, o 00BC-00BF en hexadecimal) y *SizeOfRawData* (posiciones 424-427, o 01A8-01AB en hexadecimal), colocando allí el tamaño final de la sección *text*.

Por último, se deben ajustar los campos *SizeOfImage* (posiciones 240-243, o 00F0-00F3 en hexadecimal) y *BaseOfData* (posiciones 208-211, o 00D0-00D3 en hexadecimal), con los siguientes valores obtenidos en función de *sectionAlignment* (posiciones 216-219, o 00D8-00DB en hexadecimal):

```
(2 + sizeOfCodeSection / sectionAlignment) * sectionAlignment
```

y

```
(2 + sizeOfRawData / sectionAlignment) * sectionAlignment
```

respectivamente.

A modo de ejemplo, consideremos el siguiente programa en PL/0:

CÓDIGO FUENTE	CÓDIGO TRADUCIDO CARGADO EN MEMORIA

```
var X, Y;

procedure INICIAR;
  const Y = 2;
  procedure ASIGNAR;
    X := Y;
  call ASIGNAR;

begin
  write ('NUM=');
  readln (Y);
  call INICIAR;
  writeln ('NUM*2=',Y*X)
end.
```

```
00401500   BF 7A154000           MOV EDI,0040157A
00401505   E9 17000000           JMP 00401521
0040150A   E9 0C000000           JMP 0040151B
0040150F   B8 02000000           MOV EAX,00000002
00401514   8987 00000000         MOV [EDI+00000000],EAX
0040151A   C3                    RET
0040151B   E8 EFFFFFFF           CALL 0040150F
00401520   C3                    RET
00401521   B8 30154000           MOV EAX,00401530
00401526   E8 B5FCFFFF           CALL 004011E0
0040152B   E9 05000000           JMP 00401535
00401530   4E 55 4D 3D 00        ASCII "NUM=",0
00401535   E8 56FEFFFF           CALL 00401390
0040153A   8987 04000000         MOV [EDI+00000004],EAX
00401540   E8 C5FFFFFF           CALL 0040150A
00401545   B8 54154000           MOV EAX,00401554
0040154A   E8 91FCFFFF           CALL 004011E0
0040154F   E9 07000000           JMP 0040155B
00401554   4E 55 4D 2A 32 3D 00  ASCII "NUM*2=",0
0040155B   8B87 04000000         MOV EAX,[EDI+00000004]
00401561   50                    PUSH EAX
00401562   8B87 00000000         MOV EAX,[EDI+00000000]
00401568   5B                    POP EBX
00401569   F7EB                  IMUL EBX
0040156B   E8 B0FCFFFF           CALL 00401220
00401570   E8 9BFCFFFF           CALL 00401210
00401575   E9 0EFEFFFF           JMP 00401388
```

El archivo ejecutable completo (tamaño: 2048 bytes) es el siguiente:

```
Offset      0  1  2  3  4  5  6  7   8  9  A  B  C  D  E  F

00000000   4D 5A 60 01 01 00 00 00  04 00 00 00 FF FF 00 00   MZ`.........ÿÿ..
00000010   60 01 00 00 00 00 00 00  40 00 00 00 00 00 00 00   `.......@.......
00000020   00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ................
00000030   00 00 00 00 00 00 00 00  00 00 00 00 A0 00 00 00   ............ ...
00000040   0E 1F BA 0E 00 B4 09 CD  21 B8 01 4C CD 21 54 68   ..º..´.Í!¸.LÍ!Th
00000050   69 73 20 70 72 6F 67 72  61 6D 20 69 73 20 61 20   is program is a
00000060   57 69 6E 33 32 20 63 6F  6E 73 6F 6C 65 20 61 70   Win32 console ap
00000070   70 6C 69 63 61 74 69 6F  6E 2E 20 49 74 20 63 61   plication. It ca
00000080   6E 6E 6F 74 20 62 65 20  72 75 6E 20 75 6E 64 65   nnot be run unde
00000090   72 20 4D 53 2D 44 4F 53  2E 0D 0A 24 00 00 00 00   r MS-DOS...$....
000000A0   50 45 00 00 4C 01 01 00  00 00 53 4C 00 00 00 00   PE..L.....SL....
000000B0   00 00 00 00 E0 00 02 01  0B 01 01 00 00 06 00 00   ....à...........
000000C0   00 00 00 00 00 00 00 00  00 15 00 00 00 10 00 00   ................
000000D0   00 20 00 00 00 00 40 00  00 10 00 00 00 02 00 00   . ....@.........
000000E0   04 00 00 00 00 00 00 00  04 00 00 00 00 00 00 00   ................
000000F0   00 20 00 00 00 02 00 00  00 00 00 00 03 00 00 00   . ..............
00000100   00 00 10 00 00 10 00 00  00 00 10 00 00 10 00 00   ................
00000110   00 00 00 00 10 00 00 00  00 00 00 00 00 00 00 00   ................
00000120   1C 10 00 00 28 00 00 00  00 00 00 00 00 00 00 00   ....(...........
00000130   00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ................
00000140   00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ................
00000150   00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ................
00000160   00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ................
00000170   00 00 00 00 00 00 00 00  00 10 00 00 1C 00 00 00   ................
00000180   00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ................
```

```
Offset      0  1  2  3  4  5  6  7   8  9  A  B  C  D  E  F

00000190   00 00 00 00 00 00 00 00  2E 74 65 78 74 00 00 00   .........text...
000001A0   82 05 00 00 00 10 00 00  00 06 00 00 00 02 00 00   ,...............
000001B0   00 00 00 00 00 00 00 00  00 00 00 00 20 00 00 E0   ............ ..à
000001C0   00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ................
000001D0   00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ................
000001E0   00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ................
000001F0   00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ................
00000200   6E 10 00 00 7C 10 00 00  8C 10 00 00 98 10 00 00   n...|...Œ...˜...
00000210   A4 10 00 00 B6 10 00 00  00 00 00 00 52 10 00 00   ¤...¶.......R...
00000220   00 00 00 00 00 00 00 00  44 10 00 00 00 10 00 00   ........D.......
00000230   00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ................
00000240   00 00 00 00 4B 45 52 4E  45 4C 33 32 2E 64 6C 6C   ....KERNEL32.dll
00000250   00 00 6E 10 00 00 7C 10  00 00 8C 10 00 00 98 10   ..n...|...Œ...˜.
00000260   00 00 A4 10 00 00 B6 10  00 00 00 00 00 00 00 00   ..¤...¶.........
00000270   45 78 69 74 50 72 6F 63  65 73 73 00 00 00 47 65   ExitProcess...Ge
00000280   74 53 74 64 48 61 6E 64  6C 65 00 00 00 00 52 65   tStdHandle....Re
00000290   61 64 46 69 6C 65 00 00  00 00 57 72 69 74 65 46   adFile....WriteF
000002A0   69 6C 65 00 00 00 47 65  74 43 6F 6E 73 6F 6C 65   ile...GetConsole
000002B0   4D 6F 64 65 00 00 00 00  53 65 74 43 6F 6E 73 6F   Mode....SetConso
000002C0   6C 65 4D 6F 64 65 00 00  00 00 00 00 00 00 00 00   leMode..........
000002D0   50 A2 1C 11 40 00 31 C0  03 05 2C 11 40 00 75 0D   P¢..@.1À..,.@.u.
000002E0   6A F5 FF 15 04 10 40 00  A3 2C 11 40 00 6A 00 68   jõÿ...@.£,.@.j.h
000002F0   30 11 40 00 6A 01 68 1C  11 40 00 50 FF 15 0C 10   0.@.j.h..@.Pÿ...
00000300   40 00 09 C0 75 08 6A 00  FF 15 00 10 40 00 81 3D   @..Àu.j.ÿ...@.□=
00000310   30 11 40 00 01 00 00 00  75 EC 58 C3 00 57 72 69   0.@.....uìXÃ.Wri
00000320   74 65 20 65 72 72 6F 72  00 00 00 00 00 00 00 00   te error........
00000330   00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ................
00000340   60 31 C0 03 05 CC 11 40  00 75 37 6A F6 FF 15 04   `1À..Ì.@.u7jöÿ..
00000350   10 40 00 A3 CC 11 40 00  68 D0 11 40 00 50 FF 15   .@.£Ì.@.hÐ.@.Pÿ.
00000360   10 10 40 00 80 25 D0 11  40 00 F9 FF 35 D0 11 40   ..@.€%Ð.@.ùÿ5Ð.@
00000370   00 FF 35 CC 11 40 00 FF  15 14 10 40 00 A1 CC 11   .ÿ5Ì.@.ÿ...@.¡Ì.
00000380   40 00 6A 00 68 D4 11 40  00 6A 01 68 BE 11 40 00   @.j.hÔ.@.j.h¾.@.
00000390   50 FF 15 08 10 40 00 09  C0 61 90 75 08 6A 00 FF   Pÿ...@..Àa□u.j.ÿ
000003A0   15 00 10 40 00 0F B6 05  BE 11 40 00 81 3D D4 11   ...@..¶.¾.@.□=Ô.
000003B0   40 00 01 00 00 00 74 05  B8 FF FF FF FF C3 00 52   @.....t.¸ÿÿÿÿÃ.R
000003C0   65 61 64 20 65 72 72 6F  72 00 00 00 00 00 00 00   ead error.......
000003D0   00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ................
000003E0   60 89 C6 30 C0 02 06 74  08 46 E8 E1 FE FF FF EB   `‰Æ0À..t.Fèáþÿÿë
000003F0   F2 61 90 C3 00 00 00 00  00 00 00 00 00 00 00 00   òa□Ã............
00000400   04 30 E8 C9 FE FF FF C3  00 00 00 00 00 00 00 00   .0èÉþÿÿÃ........
00000410   B0 0D E8 B9 FE FF FF B0  0A E8 B2 FE FF FF C3 00   °.è¹þÿÿ°.è²þÿÿÃ.
00000420   3D 00 00 00 80 75 4E B0  2D E8 A2 FE FF FF B0 02   =...€uN°-è¢þÿÿ°.
00000430   E8 CB FF FF FF B0 01 E8  C4 FF FF FF B0 04 E8 BD   èËÿÿÿ°.èÄÿÿÿ°.è½
00000440   FF FF FF B0 07 E8 B6 FF  FF FF B0 04 E8 AF FF FF   ÿÿÿ°.è¶ÿÿÿ°.è¯ÿÿ
00000450   FF B0 08 E8 A8 FF FF FF  B0 03 E8 A1 FF FF FF B0   ÿ°.è¨ÿÿÿ°.è¡ÿÿÿ°
00000460   06 E8 9A FF FF FF B0 04  E8 93 FF FF FF B0 08 E8   .èšÿÿÿ°.è“ÿÿÿ°.è
00000470   8C FF FF FF C3 3D 00 00  00 00 7D 0B 50 B0 2D E8   Œÿÿÿà=....}.P°-è
00000480   4C FE FF FF 58 F7 D8 3D  0A 00 00 00 0F 8C EF 00   Lþÿÿ X÷Ø=.....Œï.
00000490   00 00 3D 64 00 00 00 0F  8C D1 00 00 00 3D E8 03   ..=d....ŒÑ...=è.
000004A0   00 00 0F 8C B3 00 00 00  3D 10 27 00 00 0F 8C 95   ...Œ³...=.'...Œ•
000004B0   00 00 00 3D A0 86 01 00  7C 7B 3D 40 42 0F 00 7C   ...= †..|{=@B..|
000004C0   61 3D 80 96 98 00 7C 47  3D 00 E1 F5 05 7C 2D 3D   a=€–˜.|G=.áõ.|-=
000004D0   00 CA 9A 3B 7C 13 BA 00  00 00 00 BB 00 CA 9A 3B   .Êš;|.º....».Êš;
000004E0   F7 FB 52 E8 18 FF FF FF  58 BA 00 00 00 00 BB 00   ÷ûRè.ÿÿÿXº....».
000004F0   E1 F5 05 F7 FB 52 E8 05  FF FF FF 58 BA 00 00 00   áõ.÷ûRè.ÿÿÿXº...
00000500   00 BB 80 96 98 00 F7 FB  52 E8 F2 FE FF FF 58 BA   .»€–˜.÷ûRèòþÿÿXº
00000510   00 00 00 00 BB 40 42 0F  00 F7 FB 52 E8 DF FE FF   ....»@B..÷ûRèßþÿ
```

```
Offset      0  1  2  3  4  5  6  7   8  9  A  B  C  D  E  F

00000520   FF 58 BA 00 00 00 00 BB  A0 86 01 00 F7 FB 52 E8   ÿXº....» †..÷ûRè
00000530   CC FE FF FF 58 BA 00 00  00 00 BB 10 27 00 00 F7   ÌþÿÿXº....».'..÷
00000540   FB 52 E8 B9 FE FF FF 58  BA 00 00 00 00 BB E8 03   ûRè¹þÿÿXº....»è.
00000550   00 00 F7 FB 52 E8 A6 FE  FF FF 58 BA 00 00 00 00   ..÷ûRè¦þÿÿXº....
00000560   BB 64 00 00 00 F7 FB 52  E8 93 FE FF FF 58 BA 00   »d...÷ûRè"þÿÿXº.
00000570   00 00 00 BB 0A 00 00 00  F7 FB 52 E8 80 FE FF FF   ...»....÷ûRè€þÿÿ
00000580   58 E8 7A FE FF FF C3 00  FF 15 00 10 40 00 00 00   XèzþÿÿÃ.ÿ...@...
00000590   B9 00 00 00 00 B3 03 51  53 E8 A2 FD FF FF 5B 59   ¹....³.QSè¢ýÿÿ[Y
000005A0   3C 0D 0F 84 34 01 00 00  3C 08 0F 84 94 00 00 00   <..„4...<..„”...
000005B0   3C 2D 0F 84 09 01 00 00  3C 30 7C DB 3C 39 7F D7   <-.„....<0|Û<9□×
000005C0   2C 30 80 FB 00 74 D0 80  FB 02 75 0C 81 F9 00 00   ,0€û.tÐ€û.u.□ù..
000005D0   00 00 75 04 3C 00 74 BF  80 FB 03 75 0A 3C 00 75   ..u.<.t¿€û.u.<.u
000005E0   04 B3 00 EB 02 B3 01 81  F9 CC CC CC 0C 7F A8 81   .³.ë.³.□ùÌÌÌ.□¨□
000005F0   F9 34 33 33 F3 7C A0 88  C7 B8 0A 00 00 00 F7 E9   ù433ó| ˆÇ¸....÷é
00000600   3D 08 00 00 80 74 11 3D  F8 FF FF 7F 75 13 80 FF   =...€t.=øÿÿ□u.€ÿ
00000610   07 7E 0E E9 7F FF FF FF  80 FF 08 0F 8F 76 FF FF   .~.é□ÿÿÿ€ÿ..□vÿÿ
00000620   FF B9 00 00 00 00 88 F9  80 FB 02 74 04 01 C1 EB   ÿ¹....ˆù€û.t..Áë
00000630   03 29 C8 91 88 F8 51 53  E8 C3 FD FF FF 5B 59 E9   .)È'ˆøQSèÃýÿÿ[Yé
00000640   53 FF FF FF 80 FB 03 0F  84 4A FF FF FF 51 53 B0   Sÿÿÿ€û..„Jÿÿÿ QS°
00000650   08 E8 7A FC FF FF B0 20  E8 73 FC FF FF B0 08 E8   .èzüÿÿ° èsüÿÿ°.è
00000660   6C FC FF FF 5B 59 80 FB  00 75 07 B3 03 E9 25 FF   lüÿÿ[Y€û.u.³.é%ÿ
00000670   FF FF 80 FB 02 75 0F 81  F9 00 00 00 00 75 07 B3   ÿÿ€û.u.□ù....u.³
00000680   03 E9 11 FF FF FF 89 C8  B9 0A 00 00 00 BA 00 00   .é.ÿÿÿ‰È¹....º..
00000690   00 00 3D 00 00 00 00 7D  08 F7 D8 F7 F9 F7 D8 EB   ..=....}.÷Ø÷ù÷Øë
000006A0   02 F7 F9 89 C1 81 F9 00  00 00 00 0F 85 E6 FE FF   .÷ù‰Á□ù.....…æþÿ
000006B0   FF 80 FB 02 0F 84 DD FE  FF FF B3 03 E9 D6 FE FF   ÿ€û..„Ýþÿÿ³.éÖþÿ
000006C0   FF 80 FB 03 0F 85 CD FE  FF FF B0 2D 51 53 E8 FD   ÿ€û..…Íþÿÿ°-QSèý
000006D0   FB FF FF 5B 59 B3 02 E9  BB FE FF FF 80 FB 03 0F   ûÿÿ[Y³.é»þÿÿ€û..
000006E0   84 B2 FE FF FF 80 FB 02  75 0C 81 F9 00 00 00 00   „²þÿÿ€û.u.□ù....
000006F0   0F 84 A1 FE FF FF 51 E8  14 FD FF FF 59 89 C8 C3   .„¡þÿÿQè.ýÿÿY‰ÈÃ
00000700   BF 7A 15 40 00 E9 17 00  00 00 E9 0C 00 00 00 B8   ¿z.@.é....é....¸
00000710   02 00 00 00 89 87 00 00  00 00 C3 E8 EF FF FF FF   ....‰‡....Ãèïÿÿÿ
00000720   C3 B8 30 15 40 00 E8 B5  FC FF FF E9 05 00 00 00   Ã¸0.@.èµüÿÿé....
00000730   4E 55 4D 3D 00 E8 56 FE  FF FF 89 87 04 00 00 00   NUM=.èVþÿÿ‰‡....
00000740   E8 C5 FF FF FF B8 54 15  40 00 E8 91 FC FF FF E9   èÅÿÿÿ¸T.@.è'üÿÿé
00000750   07 00 00 00 4E 55 4D 2A  32 3D 00 8B 87 04 00 00   ....NUM*2=.‹‡...
00000760   00 50 8B 87 00 00 00 00  5B F7 EB E8 B0 FC FF FF   .P‹‡....[÷ëè°üÿÿ
00000770   E8 9B FC FF FF E9 0E FE  FF FF 00 00 00 00 00 00   è›üÿÿé.þÿÿ......
00000780   00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ................
00000790   00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ................
000007A0   00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ................
000007B0   00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ................
000007C0   00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ................
000007D0   00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ................
000007E0   00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ................
000007F0   00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ................
```

Como puede observarse comparando ambos listados, una vez que se ha cargado el programa en la memoria, las instrucciones de salto y las llamadas a subrutinas se ajustan automáticamente según los valores de las direcciones donde estén alojadas, a diferencia de los valores que se cargan en EAX y EDI para apuntar a las cadenas o las variables enteras, respectivamente, ya que éstos representan direcciones absolutas.

8. Optimización de código

La generación de código óptimo es un problema NP-completo y, por lo tanto, los llamados compiladores optimizadores por lo general producen código de alta calidad aunque no necesariamente óptimo. Al hablar de técnicas de optimización, hay que señalar que la optimización normalmente aumenta el tiempo de compilación. Por ello, el usuario muchas veces tiene la posibilidad de desactivar la parte de optimización del generador de código durante la fase de desarrollo o depuración de programas.

El código puede optimizarse en función de:

- ❒ reducir el tamaño de un programa, o
- ❒ aumentar la velocidad de ejecución de un programa.

La reducción del tamaño de un programa ya no es tan importante, gracias a la disponibilidad a precios razonables de memorias de alta capacidad, pero la optimización de la velocidad de ejecución sigue siendo de interés vital.

Las técnicas de optimización se basan en un extenso análisis de la estructura del programa y del flujo de datos. Durante la optimización suele subdividirse el programa en regiones de optimización, y las técnicas empleadas pueden categorizarse como independientes de la máquina (técnicas de carácter general) y dependientes de la máquina (técnicas para las cuales debe conocerse el hardware, ya que afectan la asignación de registros o la selección de instrucciones). Entre las técnicas de optimización están las siguientes:

8.a) Cálculo previo de constantes

Cuando aparecen varias constantes en una expresión aritmética, puede ser posible combinarlas, en el momento de la compilación, para formar una sola constante. Por ejemplo:

```
i := mayor - menor + 5
```

donde mayor = 10 y menor = 1, se puede reemplazar por:

```
i := 14
```

El efecto de esta técnica es que el código generado requiere menos memoria (porque sólo hay que almacenar una constante, en lugar de tres) y que aumenta la velocidad de ejecución del programa (porque las operaciones aritméticas se llevan a cabo durante la compilación)

8.b) Reducción de fuerza

Es el proceso por el cual una operación costosa (en términos de tiempo de ejecución) se reemplaza por una más barata. Por ejemplo, para colocar el valor cero en el registro EAX, puede preferirse la instrucción XOR EAX,EAX en lugar de MOV EAX,00000000:

```
Inst.   Operandos              Bytes
-----   -------------------    -----
MOV     registro, inmediato    5
XOR     registro, registro     2
```

```
0000  B8 00 00 00 00   MOV EAX,00000000
0005  31 C0            XOR EAX,EAX
```

La instrucción XOR EAX,EAX no solamente se ejecuta más rápido (por no usar direccionamiento inmediato), sino que además ocupa tres bytes menos que la instrucción MOV EAX,00000000.

En el siguiente ejemplo puede verse cómo una misma instrucción puede ocupar más o menos memoria. Al diseñar el compilador, esto se debe tener en cuenta.

```
0000  A1 78 56 34 12         MOV EAX,[12345678]
0005  8B 05 78 56 34 12      MOV EAX,[12345678]
000B  8B 1D 78 56 34 12      MOV EBX,[12345678]
0011  8B 0D 78 56 34 12      MOV ECX,[12345678]
0007  8B 15 78 56 34 12      MOV EDX,[12345678]
```

Otro ejemplo de reducción de fuerza es el reemplazo de multiplicaciones por potencias de dos (x*2, x*4, x*8, etc.), que pueden expresarse mediante desplazamientos aritméticos (SHR y SHL).

8.c) Reducción de frecuencia

Si un ciclo contiene cálculos que producen el mismo resultado cada vez que se ejecuta el ciclo, es posible hacer los cálculos antes de entrar al ciclo (introduciendo variables temporales, en ciertas circunstancias). Por ejemplo, en:

```
i := 0; x := 3; y := 5;
while i < 1000 do
  begin
    writeln (i+x*y);
    i := i + 1
  end;
```

se realizan 1000 multiplicaciones con el mismo resultado: 15

8.d) Optimización de ciclos

Además de la reducción de frecuencia, pueden optimizarse ciclos combinando una secuencia de ciclos con idénticos intervalos con el objetivo de generar un único ciclo, por ejemplo:

```
i := 0;
while i < 1000 do
  begin
    x := x + 2 * i;
    i := i + 1
  end;
j := 0;
while j < 1000 do
  begin
    y := y + 3 * j;
    j := j + 1
  end;
```

El programa anterior es equivalente al siguiente:

```
i := 0;
while i < 1000 do
  begin
    x := x + 2 * i;
    y := y + 3 * i;
    i := i + 1
  end;
```

8.e) Eliminación de código redundante

Aquellas secciones de código que nunca se ejecutan pueden suprimirse, por ejemplo:

```
i := 0;
while i > 0 do
  begin
  ...
  end;
```

Igualmente pueden suprimirse los términos que valgan cero en una suma, así como también la multiplicación por 1. La multiplicación por cero puede reemplazarse por una instrucción más barata.

8.f) Optimización local

Examinando grupos de instrucciones (el área local), pueden realizarse varias optimizaciones, como por ejemplo:

```
MOV EAX, EBX
MOV EBX, EAX
```

equivale a:

```
MOV EAX, EBX
```

```
E9 00 00 00 00
```

es eliminable

```
MOV EAX, 00000001
PUSH EAX
POP EAX
```

equivale a:

```
MOV EAX, 00000001
```

9. Manejo de errores

Un compilador es un sistema que en la mayoría de los casos tiene que manejar una entrada incorrecta. Sobre todo en las primeras etapas de la creación de un programa, es probable que el compilador se utilizará para efectuar las características que debería proporcionar un buen sistema de edición dirigido por la sintaxis, es decir, para determinar si las variables han sido declaradas antes de usarlas, o si faltan corchetes o algo así. Por lo tanto, el manejo de errores es parte importante de un compilador y el escritor del compilador siempre debe tener esto presente durante su diseño.

Hay que señalar que los posibles errores ya deben estar considerados al diseñar un lenguaje de programación. Por ejemplo, considerar si cada proposición del lenguaje de programación comienza con una palabra clave diferente (excepto la proposición de asignación, por supuesto). Sin embargo, es indispensable lo siguiente:

- el compilador debe ser capaz de detectar errores en la entrada;
- el compilador debe recuperarse de los errores sin perder demasiada información;
- y sobre todo, el compilador debe producir un mensaje de error que permita al programador encontrar y corregir fácilmente los elementos (sintácticamente) incorrectos de su programa.

Los mensajes de error de la forma

```
*** Error 111 ***
*** Falta declaración ***
*** Falta delimitador ***
```

no son útiles para el programador y no deben presentarse en un ambiente de compilación amigable y bien diseñado.

Por ejemplo, el mensaje de error

```
*** Falta declaración ***
```

podría reemplazarse por

```
*** No se ha declarado la variable Nombre ***
```

o en el caso del delimitador omitido se puede especificar cuál es el delimitador esperado.

Además de estos mensajes de error informativos, es deseable que el compilador produzca una lista con el código fuente e indique en ese listado dónde han ocurrido los errores.

No obstante, antes de considerar el manejo de errores en el análisis léxico y sintáctico, hay que caracterizar y clasificar los errores posibles. Esta clasificación nos mostrará que un compilador no puede detectar todos los tipos de errores.

9.a) Clasificación de errores

Durante un proceso de resolución de problemas existen varias formas en que pueden surgir errores, las cuales se reflejan en el código fuente del programa. Desde el punto de vista del compilador, los errores se pueden dividir en dos categorías:

- **errores visibles y**
- **errores invisibles.**

Los errores invisibles en un programa son aquellos que no puede detectar el compilador, ya que no son el resultado de un uso incorrecto del lenguaje de programación, sino de decisiones erróneas durante el proceso de especificación o de la mala formulación de algoritmos. Por ejemplo, si se escribe

```
a := b + c;   en lugar de   a := b * c;
```

el error no podrá ser detectado por el compilador ni por el sistema de ejecución. Estos errores lógicos no afectan la validez del programa en cuanto a su corrección sintáctica. Son objeto de técnicas formales de verificación de programas que no se consideran aquí.

Los errores visibles, a diferencia de los errores lógicos, pueden ser detectados por el compilador o al menos por el sistema de ejecución. Estos errores se pueden caracterizar de la siguiente manera:

- **errores de ortografía y**
- **errores que ocurren por omitir requisitos formales del lenguaje de programación.**

Estos errores se presentarán porque los programadores no tienen el cuidado suficiente al programar. Los errores del segundo tipo también pueden ocurrir porque el programador no comprende a la perfección el lenguaje que utiliza o porque suele escribir sus programas en otro lenguaje y, por tanto, emplea las construcciones de dicho lenguaje (estos

problemas pueden presentarse al usar a la vez lenguajes de programación como PASCAL y MODULA-2, por ejemplo).

Clasificación de ocurrencias

Por lo regular, los errores visibles o detectables por el compilador se dividen en tres clases, dependiendo de la fase del compilador en la cual se detectan:

- **errores léxicos;**
- **errores sintácticos;**
- **errores semánticos.**

Por ejemplo, un error léxico puede ocasionarse por usar un carácter inválido (uno que no pertenezca al vocabulario del lenguaje de programación) o por tratar de reconocer una constante que produce un desbordamiento.

Un error de sintaxis se detecta cuando el analizador sintáctico espera un símbolo que no corresponde al que se acaba de leer. Los analizadores sintácticos LL y LR tienen la ventaja de que pueden detectar errores sintácticos lo más pronto posible, es decir, se genera un mensaje de error en cuanto el símbolo analizado no sigue la secuencia de los símbolos analizados hasta ese momento.

Los errores semánticos corresponden a la semántica del lenguaje de programación, la cual normalmente no está descrita por la gramática. Los errores semánticos más comunes son la omisión de declaraciones.

Además de estas tres clases de errores, hay otros que serán detectados por el sistema de ejecución porque el compilador ha proporcionado el código generado con ciertas acciones para estos casos. Un error de ejecución típico ocurre cuando el índice de una matriz no es un elemento del subintervalo especificado o por intentar una división por cero. En tales situaciones, se informa del error y se detiene la ejecución del programa.

Clasificación estadística

D. G. Ripley y F. C. Druseikis investigaron los errores que cometen los programadores de PASCAL y analizaron los resultados en relación con las estrategias de recuperación. El resultado principal del estudio fue

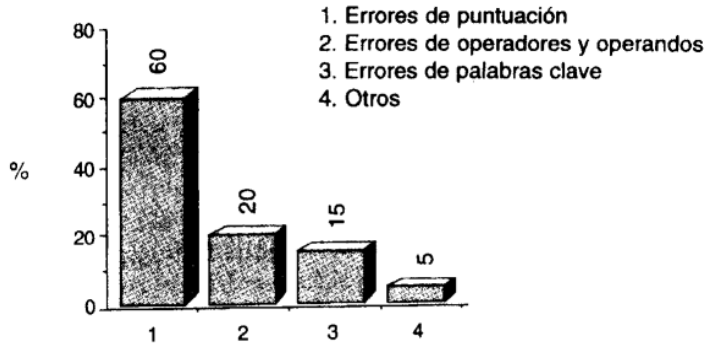
la verificación de que los errores de sintaxis suelen ser muy simples y que, por lo general, sólo ocurre un error por frase. En el resumen siguiente se describen de manera general los resultados del estudio:

- Al menos el 40% de los programas compilados eran sintáctica o semánticamente incorrectos.
- Un 80% de las proposiciones incorrectas sólo tenían un error.
- El 13% de las proposiciones incorrectas tenían dos errores, menos del 3% tenían tres errores y el resto tenían cuatro o más errores por proposición.
- En aproximadamente la mitad de los errores de componentes léxicos olvidados, el elemento que faltaba era ":", mientras que omitir el "END" final ocupaba el segundo lugar, con un 10,5%.
- En un 13% de los errores de componente léxico incorrecto se escribió "," en lugar de ";" y en más del 9% de los casos se escribió ":=" en lugar de "=".

Los errores que ocurren pueden clasificarse en cuatro categorías:

- errores de puntuación,
- errores de operadores y operandos,
- errores de palabras clave, y
- otros tipos de errores.

La distribución estadística de estas cuatro categorías aparece en la siguiente figura:



Distribución estadística de las categorías de errores

9.b) Efectos de los errores

La detección de un error en el código fuente ocasiona ciertas reacciones del compilador.

El comportamiento de un compilador en el caso de que el código fuente contenga un error puede tener varias facetas:

- **El proceso de compilación se detiene al ocurrir el error y el compilador debe informar del error.**
- **El proceso de compilación continúa cuando ocurre el error y se informa de éste en un archivo de listado.**
- **El compilador no reconoce el error y por tanto no advierte al programador.**

La última situación nunca debe presentarse en un buen sistema de compilación; es decir, el compilador debe ser capaz de detectar todos los errores visibles.

La detención del proceso de compilación al detectar el primer error es la forma más simple de satisfacer el requisito de que una compilación siempre debe terminar sin importar cuál sea la entrada. Sin embargo, este comportamiento también es el peor en un ambiente amigable para el usuario, ya que una compilación puede demorar algún tiempo. Por lo tanto, el programador espera que el sistema de compilación detecte todos los errores posibles en el mismo proceso de compilación.

Entonces, en general, el compilador debe recuperarse de un error para poder revisar el código fuente en busca de otros errores. No obstante, hay que observar que cualquier "reparación" efectuada por el compilador tiene el propósito único de continuar la búsqueda de otros errores, no de corregir el código fuente. No hay reglas generales bien definidas acerca de cómo recuperarse de un error, por lo cual el proceso de recuperación debe basarse en hipótesis acerca de los errores. La carencia de tales reglas se debe al hecho de que el proceso de recuperación siempre depende del lenguaje.

9.c) Manejo de errores en el análisis léxico

Los errores léxicos se detectan cuando el analizador léxico intenta reconocer componentes léxicos en el código fuente. Los errores léxicos típicos son:

- nombres ilegales de identificadores: un nombre contiene caracteres inválidos;
- números inválidos: un número contiene caracteres inválidos (por ejemplo, 2,13 en lugar de 2.13), no está formado correctamente (por ejemplo, 0.1.33), o es demasiado grande y por tanto produce un desbordamiento;
- cadenas incorrectas de caracteres: una cadena de caracteres es demasiado larga (probablemente por la omisión de comillas que cierran);
- errores de ortografía en palabras reservadas: caracteres omitidos, adicionales, incorrectos o mezclados;
- fin de archivo: se detecta un fin de archivo a la mitad de un componente léxico.

La mayoría de los errores léxicos se deben a descuidos del programador. En general, la recuperación de los errores léxicos es relativamente sencilla.

Si un nombre, un número o una etiqueta contiene un carácter inválido, se elimina el carácter y continúa el análisis en el siguiente carácter; en otras palabras, el analizador léxico comienza a reconocer el siguiente componente léxico. El efecto es la generación de un error de sintaxis que será detectado por el analizador sintáctico. Este método también puede aplicarse a números mal formados.

Las secuencias de caracteres como 12AB pueden ocurrir si falta un operador (el caso menos probable) o cuando se han tecleado mal ciertos caracteres. Es imposible que el analizador léxico pueda decidir si esta secuencia es un identificador ilegal o un número ilegal. En tales casos, el analizador léxico puede saltarse la cadena completa o intentar dividir las secuencias ilegales en secuencias legales más cortas. Independientemente de cuál sea la decisión, la consecuencia será un error de sintaxis.

La detección de cadenas demasiado largas no es muy complicada, incluso si faltan las comillas que cierran, porque por lo general no está permitido que las cadenas pasen de una línea a la siguiente. Si faltan las comillas que cierran, puede usarse el carácter de fin de línea como el fin de la cadena y reanudar el análisis léxico en la línea siguiente. Esta reparación quizás produzca errores adicionales. En cualquier caso, el programador debe ser informado por medio de un mensaje de error.

Un caso similar a la falta de comillas que cierran en una cadena, es la falta de un símbolo de terminación de comentario. Como por lo regular está permitido que los comentarios abarquen varias líneas, no podrá detectarse la falta del símbolo que cierra el comentario hasta que el analizador léxico llegue al final del archivo o al símbolo de fin de otro comentario (si no se permiten comentarios anidados).

Si se sabe que el siguiente componente léxico debe ser una palabra reservada, es posible mediante funciones de corrección de errores corregir una palabra reservada mal escrita, aplicando una función de distancia métrica entre la entrada y el conjunto de palabras reservadas.

Por último, el proceso de compilación puede terminar si se detecta un fin de archivo dentro de un componente léxico.

9.d) Manejo de errores en el análisis sintáctico

El analizador sintáctico detecta un error de sintaxis cuando el analizador léxico proporciona el siguiente símbolo y éste es incompatible con el estado actual del analizador sintáctico. Los errores sintácticos típicos son:

- **paréntesis o corchetes omitidos, por ejemplo, `x := y * (1 + z;`**
- **operadores u operandos omitidos, por ejemplo, `x := y (1 + z);`**
- **delimitadores omitidos, por ejemplo, `x := y IF a > x THEN y := z;`**

No hay estrategias de recuperación de errores cuya validez sea general, y la mayoría de las estrategias conocidas son heurísticas, ya que se basan en suposiciones acerca de cómo pueden ocurrir los errores y lo que probablemente quiso decir el programador con una determinada construcción. Sin embargo, hay algunas estrategias que gozan de amplia aceptación:

- **Recuperación de emergencia (o en modo pánico): Al detectar un error, el analizador sintáctico salta todos los símbolos de entrada hasta encontar un símbolo que pertenezca a un conjunto previamente definido de símbolos de sincronización. Estos símbolos de sincronización son el punto y coma, el símbolo *end* o cualquier palabra clave que pueda ser el inicio de una proposición nueva, por ejemplo. Es fácil implantar la recuperación de emergencia, pero sólo reconoce un error por proposición. Esto no necesariamente es una desventaja, ya que no es muy probable que ocurran varios errores en la misma proposición. Esta**

suposición es un ejemplo típico del carácter heurístico de esta estrategia.

- Recuperación por inserción, borrado y reemplazo: Éste también es un método fácil de implantar y funciona bien en ciertos casos de error. Usemos como ejemplo una declaración de variable en PASCAL. Cuando una coma va seguida por dos puntos, en lugar de un nombre de variable, es posible eliminar esta coma.
- Recuperación por expansión de gramática: el 60% de los errores en los programas fuente son errores de puntuación, por ejemplo, la escritura de un punto y coma en lugar de una coma, o viceversa. Una forma de recuperarse de estos errores es legalizarlos en ciertos casos, introduciendo lo que llamaremos producciones de error en la gramática del lenguaje de programación. La expansión de la gramática con estas producciones no quiere decir que ciertos errores no serán detectados, ya que pueden incluirse acciones para informar de su detección.

La recuperación de emergencia es la estrategia que se encontrará en la mayoría de los compiladores, pero también la legalización de ciertos errores mediante la definición de una gramática aumentada es una técnica que se emplea con frecuencia. No obstante, hay que expandir la gramática con mucho cuidado para asegurarse de que no cambien el tipo y las características de la gramática.

9.e) Errores semánticos

Los errores que puede detectar el analizador sintáctico son aquellos que violan las reglas de una gramática independiente del contexto. Algunas de las características de un lenguaje de programación no pueden enunciarse con reglas independientes del contexto, ya que dependen de él; por ejemplo, la restricción de que los identificadores deben declararse previamente. Por lo tanto, los principales errores semánticos son:

- identificadores no definidos;
- operadores y operandos incompatibles.

Es mucho más difícil introducir métodos formales para la recuperación de errores semánticos que para la recuperación de errores sintácticos, ya que a menudo la recuperación de errores semánticos es *ad hoc*. No obstante, puede requerirse que, por lo menos, el error semántico sea informado al programador y que se suprima la generación de código.

Sin embargo, la mayoría de los errores semánticos pueden ser detectados mediante la revisión de la tabla de símbolos. Si se detecta un identificador no definido, es conveniente insertar el identificador en la tabla de símbolos, suponiendo un tipo que se base en el contexto donde ocurra o un tipo universal que permita al identificador ser un operando de cualquier operador del lenguaje. Al hacerlo, evitamos la producción de un mensaje de error cada vez que se use la variable no definida. Si el tipo de un operando no concuerda con los requisitos de tipo del operador, también es conveniente reemplazar el operando con una variable ficticia de tipo universal.

10. Bibliografía

Aho, A. et al.: "Compiladores. Principios, técnicas y herramientas", Pearson, 2da. Edición, 2008

Louden, K.: "Construcción de compiladores. Principios y prácticas", Thomson International, México, 2004

Microsoft Corporation: "Microsoft Portable Executable and Common Object File Format Specification – Revision 8.1 – February 15, 2008", en: http://www.microsoft.com/whdc/system/platform/firmware/PECOFF.mspx

Teufel, B. et al.: "Compiladores. Conceptos Fundamentales", Addison-Wesley Iberoamericana, México, 1995

Wirth, N.: "Algorithms + Data Structures = Programs", Prentice-Hall, Englewood Cliffs, 1976

11. Otros recursos sugeridos

***Depurador OllyDbg*: http://www.ollydbg.de**
***Depurador Syser*: http://www.sysersoft.com**
***Desensamblador IDA Pro*: http://www.hex-rays.com/idapro**
***Editor Notepad++*: http://www.notepad-plus-plus.org**
(*Plugin Hex Editor*: http://sourceforge.net/projects/npp-plugins/files/Hex%20Editor)
***Identificador PEiD*: http://www.peid.info**