B0B99PRPA – Procedurální programování

Ukazatele a práce s pamětí, ladění

Stanislav Vítek

Katedra radioelektroniky
Fakulta elektrotechnická
České vysoké učení v Praze

Přehled témat

- Část 1 – Ukazatele, pole v dynamické paměti
  - Modifikátor const
  - 2D pole v dynamické paměti
- Část 2 – Práce s pamětí, pamětové třídy
  - Výpočetní prostředky, paměť
  - Rozsah platnosti proměnných
  - Ukazatele na funkci
- Část 3 – Ladění
  - GDB
  - Valgrind
- Část 4 – Zadání 5. domácího úkolu

Část I

Ukazatele a práce s pamětí

I. Ukazatele a práce s pamětí

Modifikátor `const`

- Uvedením klíčového slova const můžeme označit proměnnou jako konstantu
  - Překladač kontroluje přiřazení
- Pro definici konstant můžeme použít např.

```
const float pi = 3.14159265;
```

- Na rozdíl od symbolické konstanty

```
#define PI 3.14159265
```

  - mají konstantní proměnné typ
  - překladač tak může provádět typovou kontrolu

Ukazatele na konst. proměnné a konst. ukazatele

- Klíčové slovo `const` můžeme zapsat před jméno typu nebo před jméno proměnné
- Dostáváme 3 možnosti jak definovat ukazatel s `const`
  1. `const int *ptr;` – ukazatel na konstantní proměnnou
     - Nemůžeme použít pointer pro změnu hodnoty proměnné
     - `const int *` lze též zapsat jako `int const *`
  2. `int *const ptr;` – konstantní ukazatel
     - Pointer nemůžeme nastavit na jinou adresu než tu při inicializaci
  3. `const int *const ptr;` – konstantní ukazatel na konstantní hodnotu
     - Kombinuje předchozí dva případy
     - `const int * const` lze též zapsat jako `int const * const`

Ukazatel na konstantní proměnnou (hodnotu)

- Prostřednictvím ukazatele na konstantní proměnnou nelze tuto proměnnou měnit

```
int v = 10;
int v2 = 20;
const int *ptr = &v;
printf("*ptr: %d\n", *ptr);
*ptr = 11;  /* NELZE! */
v = 11;     /* lze menit promennou */
printf("*ptr: %d\n", *ptr);
ptr = &v2; /* lze priradit novou adresu ukazateli */
printf("*ptr: %d\n", *ptr);
```

Konstatní ukazatel

- Hodnotu konstantního ukazatele nelze po inicializaci měnit
- Zápis `int *const ptr;` můžeme číst zprava doleva
  - `ptr` – proměnná, která je `*const` – konstantním ukazatelem
  - `int` – na proměnnou typu int

```
int v = 10;
int v2 = 20;
int *const ptr = &v;
printf("v: %d *ptr: %d\n", v, *ptr);
*ptr = 11; /* lze zmenit odkazovanou promennou */
printf("v: %d\n", v);
ptr = &v2; /* NELZE! */
```

Konstantní ukazatel na konstantní proměnnou

- Hodnotu konstantního ukazatele na konstantního proměnnou nelze po inicializaci měnit a ani nelze prostřednictvím takového ukazatele měnit hodnotu adresované proměnné.
- Zápis `const int *const ptr;` můžeme číst zprava doleva
  - `ptr` – proměnná, která je `*const` – konstantním ukazatelem
  - `const int` – na proměnnou typu const int

```
int v = 10;
int v2 = 20;
const int *const ptr = &v;
printf("v: %d *ptr: %d\n", v, *ptr);
ptr = &v2; /* NELZE! */
*ptr = 11; /* NELZE! */
```

I. Ukazatele a práce s pamětí

Modifikátor const

2D pole v dynamické paměti

2D pole v dynamické paměti

- Pole ukazatelů na jednotlivé řádky pole
  - nelze měnit počet řádků
  - délka řádků může být různá

```
int *p[2];
/* prvni radek */
p[0] = (int *)malloc (3*sizeof(int));
/* druhy radek */
p[1] = (int *)malloc (3*sizeof(int));
```

2D pole v dynamické paměti

- Ukazatel na ukazatel
  - lze měnit počet řádků délka řádků může být různá

```
int ** p;
p = (int **)malloc (2*sizeof(int));
p[0] = (int *)malloc (3*sizeof(int));
p[1] = (int *)malloc (3*sizeof(int));
```

- Ukazatel na N-prvkové pole
  - ekvivalent pole ve statické paměti

```
int (*p)[3];
/* alokujeme souvisly blok 6 prvku */
p = (int (*)[3])malloc (6*sizeof(int));
```

Část II

Práce s pamětí, paměťové třídy

II. Práce s pamětí, paměťové třídy

Rozdělení paměti

1. **Zásobník**
   - lokální proměnné, argumenty funkcí, návratová hodnota funkce
   - spravováno automaticky
2. **Halda**
   - dynamická paměť (malloc(), free())
   - spravuje programátor
3. **Statická**
   - globální nebo "lokální" static proměnné
   - inicializace při startu
4. **Literály**
   - hodnoty zapsané ve zdrojovém kódu programu, např. textové řetězce
   - inicializace při startu, READ ONLY
5. **Program**
   - strojové instrukce
   - inicializace při startu

Přidělování paměti proměnným

- Určení paměťového místa pro uložení hodnoty proměnné v paměti
- Lokálním proměnným a parametrům funkce se paměť přiděluje při volání funkce
  - Paměť zůstane přidělena jen do návratu z funkce
  - Paměť se automaticky alokuje z rezervovaného místa – zásobník
  - Při návratu funkce se přidělené paměťové místo uvolní
  - Výjimku tvoří lokální proměnné s modifikátorem static
    - Z hlediska platnosti rozsahu mají charakter lokálních proměnných
    - Jejich hodnota je však zachována i po skončení funkce / bloku
    - Jsou umístěny ve statické části paměti
- Dynamické přidělování paměti
  - Alokace paměti se provádí funkcí `malloc()`
  - Paměť se alokuje z rezervovaného místa – halda

Zásobník

- Úseky paměti přidělované lokálním proměnným a parametrům
  - Úseky se přidávají a odebírají
  - Vždy se odebere naposledy přidaný úsek – LIFO (last in, first out)
  - Na zásobník se ukládá "volání funkce"
- Na zásobník se ukládá
  - návratová hodnota funkce
  - hodnota čítače programu před voláním funkce
- Ze zásobníku se alokují proměnné parametrů funkce
  - Argumenty (parametry) jsou de facto lokální proměnné
  - Opakovaným rekurzivním voláním funkce můžeme zaplnit velikost přiděleného zásobníku program skončí chybou.

Rekurzivní volání funkce

```
#include <stdio.h>
void funkce(int v)
{
  printf("hodnota: %i\n", v);
  funkce(v + 1);
}
int main(void)
{
  funkce(1);
}
```

- Vyzkoušejte si program pro omezenou velkost zásobníku

  ```
  $ ulimit -s 1000
  ```

Proměnná

Vymezená oblast paměti a v C je můžeme rozdělit podle způsobu alokace

- **Statická alokace** – provede se při deklaraci statické nebo globální proměnné.
  - Paměťový prostor je alokován při startu programu a nikdy není uvolněn.
- **Automatická alokace**
  - probíhá automaticky v případě lokálních proměnných (nebo argumentů funkce)
  - paměťový prostor je alokován na zásobníku a paměť proměnné je automaticky uvolněna s koncem platnosti proměnné. např. po ukončení bloku funkce.
- **Dynamická alokace**
  - není podporována přímo jazykem C, ale je přístupná knihovními funkcemi (stdlib, malloc)

Paměťové třídy

- **auto** (lokální)
  - definuje proměnnou jako dočasnou (automatickou)
  - typicky lokální proměnná deklarovaná uvnitř funkce
  - implicitní nastavení, platnost proměnné je omezena na blok
  - proměnná je v zásobníku.
- **register**
  - doporučuje překladači umístit proměnnou do registru procesoru.
  - překladač může, ale nemusí vyhovět
  - nelze ziskat adresu
  - jinak stejné jako auto
- **static**
  - **uvnitř bloku** – proměnnou je statická – ponechává si hodnotu i při opuštění bloku. Je uložena v datové oblasti.
  - **vně bloku** – kde je implicitně proměnná uložena v datové oblasti (statická) omezuje její viditelnost na modul.
- **extern**
  - rozšiřuje viditelnost statických proměnných z modulu na celý program
  - globální proměnné s extern jsou definované v datové oblasti

Příklad deklarace proměnných

```
// program.h
extern int globalni;  // deklarace
                      // extern int globalni = 10; by bylo definici

// program.c
int globalni = 10;

void funkce() {
  int lokalni = 0;    // lokalni promenna
  int statlok = 0;    // staticka lokalni promenna
  printf("lokalni: %d, staticka: %d\n", ++lokalni, ++statlok);
}

int main() {
  funkce();
  funkce();
  funkce();
}
```

II. Práce s pamětí, paměťové třídy

Rozsah platnosti proměnných

```
int a = 10;      // globalni promenna
int main () {    // začátek bloku 1
int a = 100;  // lokalni promenna, zastini globalni
{              // zacatek bloku 2
int a = 1, b = 2;
a +=  b;     // vysledek?
}              // konec bloku 2
b = 20;        // promenna b nena platna
}
```

- Globální proměnné mají rozsah platnosti kdekoliv“ v programu
- Zastíněný přístup lze řešit modifikátorem `extern` (v novém bloku)

Definice vs. deklarace

- platí pro proměnné i funkce
- definice je přidělení paměťového místa
- deklarace je oznámení, že proměnná (funkce) je někde definována
- Zřejmě:
  - definici je možné provést pouze jednou
  - pokus o vícenásobnou definici skončí chybou překladu (linkování) programu

Definice vs. deklarace

```
// definice.h
int global = 5;
int funkce (int);

// definice.c
#include "definice.h"
static int modul;

int funkce (int a)
{
printf ("arg: %d, global: %
  d", a, global);
return 0;
}
```

```
#include "definice.h"

int main ()
{
global += 1;
funkce (1);
funkce (1);
global += 1;
funkce (1);
return 0;
}
```

II. Práce s pamětí, paměťové třídy

Ukazatele na funkci

- Definice (implementace) funkce je umístěna někde v paměti.
  - podobně jako v případě proměnné můžeme deklarovat ukazatel na funkci
  - ukazatel lze využít k dynamickému volání funkce (podle hodnoty ukazatele)
  - součástí volání funkce jsou argumenty
    - jejich datový typ je součástí ukazatele.
- Funkce (a volání funkce) je identifikátor funkce a (), tj.

```
typ_návratové_hodnoty funkce(argumenty funkce);
```

- Ukazatel na funkci definujeme jako

```
typ_návratové_hodnoty (*ukazatel)(argumenty funkce)
```

Ukazatele na funkci – příklad

- Používáme derefenční operátor, jako u ukazatele na proměnnou

```
1  #include <stdio.h>
2
3  void funkce (int a) {
4          printf ("%d\n", a);
5  }
6  int main () {
7          void (*ukazatel)(int);
8          ukazatel = funkce;
9          (*ukazatel)(10);
10         return 0;
11 }
```

Definice typu – typedef

- Operátor typedef umožňuje definovat nový datový typ
- Slouží k pojmenování typů, např. ukazatele, struktury a uniony
- Například typ pro ukazatele na double a nové jméno pro int:

```
typedef double* double_p;
typedef int integer;
double_p x, y;              // totozne s double *x,
    *y;
integer i, j;              // totozne s int i, j;
```

  - Zavedením typů operátorem typedef umožňuje používání nových jmen typů v celém programu
  - Výhoda zavedení nových typů je především u složitějších typů – ukazatele na funkce nebo struktury

Část III

Ladění

III. Ladění

GDB

Valgrind

GDB – spuštění

- řádkově orientovaný debugger
- existuje grafická nadstavba **ddd** a semigrafické **gdbtui**
- je třeba kompilovat s debugovacími symboly (`-g`)

```
int main()
{
  int i = 1337;
  return 0;
}
```

```
$ gcc -g program.c
$ gdb ./a.out
```

Než pořádně začneme

```
(gdb) print 1 + 2
$1 = 3

(gbd) print (int) 2147483648
$2 = -2147483648
```

GDB – základní příkazy

run – spustí běh

list – ukáže 10 řádků kódu

break [název funkce nebo číslo řádku] – nastaví breakpoint

clear [název funkce nebo číslo řádku] – smaže breakpoint

info break – zobrazí seznam breakpointů

step – provede jeden krok program (zkratka s)

step [počet kroků] – provede uvedený počet kroků programu

backtrace – vypíšte backtrace

info locals – zobrazí lokální proměnné

info args – zobrazí argumenty rámce

info variables – zobrazí všechny statické a globální proměnné

info functions – zobrazí všechny definované funkce

GDB - základní práce, nastavení breakpointů

```
(gdb) break main
(gdb) run
```

Program se zastavil na řádce 3, těsně před inicializací proměnné i

---

```
(gdb) print i
$3 = 32767
```

Výpis obecně náhodné hodnoty

```
(gdb) next
(gdb) print i
$4 = 1337
```

Posun o jeden řádek, proměnná i je již inicializovaná

GDB – inspekce paměti

```
(gdb) print &i
$5 = (int *) 0x7fff5fbff584
(gdb) print sizeof(i)
$6 = 4
```

Zjevně disponuji strojem, kde má int 4 byty

```
(gdb) x/4xb &i
0x7fff5fbff584:  0x39 0x05 0x00 0x00
```

4 bajty od adresy &i, little endian!

```
(gdb) set var i = 0x12345678
(gdb) x/4xb &i
0x7fff5fbff584:  0x78 0x56 0x34 0x12
```

GDB – inspekce datových typů

```
(gdb) ptype i
type = int

(gdb) ptype &i
type = int *

(gdb) ptype main
type = int (void)
```

GDB - pole a ukazatele

```
int main()
{
  int a[] = {1,2,3};
  return 0;
}
```

```
(gdb) break main
(gdb) run
(gdb) next
```

```
(gdb) print a
$1 = 1, 2, 3

(gdb) ptype a
type = int [3]

(gdb) x/12xb &a
0x7fff5fbff56c:  0x01 0x00
0x00 0x00 0x02 0x00 0x00 0x00
0x7fff5fbff574:  0x03 0x00
0x00 0x00
```

GDB - pole a ukazatele

```
(gdb) print a[0]
$4 = 1

(gdb) print *(a + 0)
$5 = 1

(gdb) print a[1]
$6 = 2

(gdb) print *(a + 1)
$7 = 2

(gdb) print a[2]
$8 = 3

(gdb) print *(a + 2)
$9 = 3
```

```
(gdb) ptype &a
type = int (*)[3]

(gdb) print a + 1
$10 = (int *) 0x7fff5fbff570

(gdb) print &a + 1
$11 = (int (*)[3]) 0x7fff5fbff578

(gdb) print &a[0]
$11 = (int *) 0x7fff5fbff56c
```

GDB – složitější případ

```
1  #include <stdio.h>
2
3  short f(short n)
4  {
5    if (n==0 || n==1)
6      return 1;
7    return n*f(n-1);
8  }
9
10 int main(void)
11 {
12   printf("%d\n", f
       (8));
13   return 0;
14 }
```

```
(gdb) list
```

Výpis části zdrojového kódu

```
(gdb) break factorial
```

Nastavení breakpointu

```
(gdb) run
(gdb) print(n)
$1 = 8
```

Spuštění programu a výpis parametru funkce

```
(gdb) continue
Continuing.
(gdb) print(n)
$2 = 7
```

Pokračování v běhu a opětovný výpis parametru

```
(gdb) clear main
Deleted breakpoint 1
(gdb) run
```

Odstranění breakpointu

GDB – složitější případ

```
1  #include <stdio.h>
2
3  short f(short n)
4  {
5    if (n==0 || n==1)
6      return 1;
7    return n*f(n-1);
8  }
9
10 int main(void)
11 {
12   printf("%d\n", f
       (8));
13   return 0;
14 }
```

```
(gdb) break factorial
```

breakpoint na vstupní bod funkce nazvané `f`

```
(gdb) info breakpoints
```

získáme informaci o všech breakpointech

```
(gdb) ignore 1 5
(gdb) r
```

breakpoint ignoruje prvních pět průchodů

```
(gdb) bt
```

historie volání – backtrace, zkratka bt

```
(gdb) bt 4
```

zajímá nás jen část

III. Ladění

GDB

Valgrind

Valgrind

- Dynamická analýza kódu
- Detekce
  - podmíněných skoků závislých na neinicializované proměnné
  - neoprávněné čtení / zápis do paměti
  - neuvolňování paměti (memory leak)

Část IV

Zadání 5. domácího úkolu

Zadání 5. domácího úkolu (HW05)

Téma: **Zpracování číselné řady**

- **Motivace:** Práce s polem v dynamické paměti
- **Cíl:** Zpracování teoreticky neomezeně dlouhé řady celých čísel
- **Zadání:** `https://cw.fel.cvut.cz/wiki/courses/b0b99prpa/hw/hw05`
  - Načtení předem neznámého počtu vstupních hodnot
  - Výpočet standardních statistických ukazatelů – medián, histogram
- **Termín odevzdání:** **17.11.2018, 23:59:59**

Shrnutí přednášky

Diskutovaná témata

- 2D pole v dynamické paměti
- Rozdělení paměti
- Rozsah platnosti proměnných
- Ladící prostředky

- Příště: struktury, reprezentace čísel v počítači

Diskutovaná témata

- 2D pole v dynamické paměti
- Rozdělení paměti
- Rozsah platnosti proměnných
- Ladící prostředky

- Příště: struktury, reprezentace čísel v počítači