А.В. Макаров, С.Ю. Скоробогатов, А.М. Чеповский

Учебный курс “CIL и системное программирование в Microsoft .NET”

Лекция 9.

Язык CIL: инструкции общего назначения

Введение

- Инструкции общего назначения служат для организации вычислений
- Категории инструкций общего назначения:
  - Инструкции для загрузки и сохранения значений
  - Арифметические инструкции
  - Инструкции для организации передачи управления

9.1. Инструкции для загрузки и сохранения значений

- Выполняют копирование значений на стек вычислений и сохранение значений со стека вычислений в память

9.1.1. Загрузка констант

Код	Инструкция	Встроенный операнд	Описание
0x14	**ldnull**	–	Загрузка константы null
0x15	**ldc.**m1	–	Загрузка целого числа -1 (int32)
0x16 – 0x1E	**ldc.**0 - **ldc.**8	–	Загрузка целых чисел от 0 до 8 (int32)
0x1F	**ldc.**s	int8	Загрузка целых чисел от -128 до 127 (int32)
0x20	**ldc.**i4	int32	Загрузка целых чисел (int32)
0x21	**ldc.**i8	int64	Загрузка целых чисел (int64)
0x22	**ldc.**r4	float32	Загрузка чисел с плавающей запятой (F)
0x23	**ldc.**r8	float64	Загрузка чисел с плавающей запятой (F)

- Диаграмма стека:

  … **->** … **, constant**

9.1.2. Работа с переменными и параметрами методов

- Локальные переменные и параметры имеют номера от 0 до 65534
- Существуют три варианта инструкций для работы с переменными и параметрами:
  - Сокращенные инструкции, работающие с переменными и параметрами, имеющими номера от 0 до 3
  - Сокращенные инструкции, допускающие номера переменных и параметров от 0 до 255
  - Обычные инструкции, работающие с любыми переменными и параметрами

Инструкции для загрузки параметров и локальных переменных

Код	Инструкция	Встроенный операнд	Описание
0x02 – 0x05	**ldarg.**0 – **ldarg.**3	–	Загрузка параметров с номерами от 0 до 3
0x06 – 0x09	**ldloc.**0 – **ldloc.**3	–	Загрузка локальных переменных с номерами от 0 до 3
0x0E	**ldarg.**s	unsigned int8	Загрузка параметров с номерами от 0 до 255
0x11	**ldloc.**s	unsigned int8	Загрузка локальных переменных с номерами от 0 до 255
0xFE 0x09	**ldarg**	unsigned int16	Загрузка параметров с номерами от 0 до 65534
0xFE 0x0C	**ldloc**	unsigned int16	Загрузка локальных переменных с номерами от 0 до 65534

- Диаграмма стека:

  … **->** … **, value**

Инструкции для загрузки адресов параметров и локальных переменных

Код	Инструкция	Встроенный операнд	Описание
0x0F	**`ldarga.`**`s`	unsigned int8	Загрузка адресов параметров с номерами от 0 до 255
0x12	**`ldloca.`**`s`	unsigned int8	Загрузка адресов локальных переменных с номерами от 0 до 255
0xFE 0x0A	**`ldarga`**	unsigned int16	Загрузка адресов параметров с номерами от 0 до 65534
0xFE 0x0D	**`ldloca`**	unsigned int16	Загрузка адресов локальных переменных с номерами от 0 до 65534

- Диаграмма стека:

  … **`->`** … **`, address`**

Инструкции для сохранения значений в параметрах и локальных переменных

Код	Инструкция	Встроенный операнд	Описание
0x0A – 0x0D	**stloc.**0 – **stloc.**3	–	Сохранение значений в локальных переменных с номерами от 0 до 3
0x10	**starg.**s	unsigned int8	Сохранение значений в параметрах с номерами от 0 до 255
0x13	**stloc.**s	unsigned int8	Сохранение значений в локальных переменных с номерами от 0 до 255
0xFE 0x0B	**starg**	unsigned int16	Сохранение значений в параметрах с номерами от 0 до 65534
0xFE 0x0E	**stloc**	unsigned int16	Сохранение значений в локальных переменных с номерами от 0 до 65534

- Диаграмма стека:

  … , **value ->** …

9.1.3. Косвенная загрузка и сохранение значений

- При косвенной загрузке и сохранении значений работа с памятью осуществляется через адреса (управляемые и неуправляемые указатели)
- Диаграмма стека в случае загрузки значения:

  … , **address** -> … , **value**

- Диаграмма стека в случае сохранения значения:

  … , **address, value** -> …

Инструкции для косвенной загрузки значений

Код	Инструкция	Встроенный операнд	Описание
0x46	**ldind.**i1	–	Косвенная загрузка значения int8
0x47	**ldind.**u1	–	Косвенная загрузка значения unsigned int8
0x48	**ldind.**i2	–	Косвенная загрузка значения int16
0x49	**ldind.**u2	–	Косвенная загрузка значения unsigned int16
0x4A	**ldind.**i4	–	Косвенная загрузка значения int32
0x4B	**ldind.**u4	–	Косвенная загрузка значения unsigned int32
0x4C	**ldind.**i8 (**ldind.**u8)	–	Косвенная загрузка значения int64 и unsigned int64
0x4D	**ldind.**i	–	Косвенная загрузка значения native int
0x4E	**ldind.**r4	–	Косвенная загрузка значения float32
0x4F	**ldind.**r8	–	Косвенная загрузка значения float64
0x50	**ldind.**ref	–	Косвенная загрузка объектной ссылки

Инструкции для косвенного сохранения значений

Код	Инструкция	Встроенный операнд	Описание
0x51	**stind.**ref	–	Косвенное сохранение объектной ссылки
0x52	**stind.**i1	–	Косвенное сохранение значения int8
0x53	**stind.**i2	–	Косвенное сохранение значения int16
0x54	**stind.**i4	–	Косвенное сохранение значения int32
0x55	**stind.**i8	–	Косвенное сохранение значения int64
0x56	**stind.**r4	–	Косвенное сохранение значения float32
0x57	**stind.**r8	–	Косвенное сохранение значения float64
0xDF	**stind.**i	–	Косвенное сохранение значения native int

9.1.4. Специальные инструкции для работы со стеком

Код	Инструкция	Встроенный операнд	Описание
0x25	**dup**	–	Копирование значения на вершине стека
0x26	**pop**	–	Удаление значения с вершины стека

- Диаграмма стека для инструкции dup:

  … , **value** -> …, **value, value**

- Диаграмма стека для инструкции pop:

  … , **value** -> …

9.2. Арифметические инструкции

- Категории арифметических инструкций:
  - Бинарные операции: …, **value1, value2 -> …, result**
  - Унарные операции: …, **value -> …, result**
  - Инструкция ckfinite, проверяющая конечность значений с плавающей точкой: …, **value -> …, value**
  - Инструкции преобразования значений:

    …, **value -> …, result**

Базовые бинарные арифметические операции

Код	Инструкция	Встроенный операнд	Описание
0x58	**add**	–	Сложение
0x59	**sub**	–	Вычитание
0x5A	**mul**	–	Умножение
0x5B	**div**	–	Деление
0x5C	**div.**un	–	Деление беззнаковых целых чисел
0x5D	**rem**	–	Остаток от деления
0x5E	**rem.**un	–	Остаток от деления беззнаковых целых чисел
0x5F	**and**	–	Побитовое И
0x60	**or**	–	Побитовое ИЛИ
0x61	**xor**	–	Побитовое ИСКЛЮЧАЮЩЕЕ ИЛИ

Бинарные арифметические операции с контролем переполнения

Код	Инструкция	Встроенный операнд	Описание
0xD6	**add**.ovf	–	Сложение целых чисел со знаком с контролем переполнения
0xD7	**add**.ovf.un	–	Сложение целых чисел без знака с контролем переполнения
0xD8	**mul**.ovf	–	Умножение целых чисел со знаком с контролем переполнения
0xD9	**mul**.ovf.un	–	Умножение целых чисел без знака с контролем переполнения
0xDA	**sub**.ovf	–	Вычитание целых чисел со знаком с контролем переполнения
0xDB	**sub**.ovf.un	–	Вычитание целых чисел без знака с контролем переполнения

Операции сдвига

Код	Инструкция	Встроенный операнд	Описание
0x62	**shl**	–	Сдвиг целых чисел влево
0x63	**shr**	–	Сдвиг целых чисел со знаком вправо
0x64	**shr**.un	–	Сдвиг целых чисел без знака вправо

- Диаграмма стека:

  …, **value, shift** -> …, **result**

Операции сравнения

- Операции выполняют сравнение значений своих операндов. Результатом сравнения являются числа 0 или 1 (типа int32)
- Семантика операций сравнения для чисел с плавающей запятой существенно отличается от их семантики для целых чисел:
  - числа с плавающей запятой могут дополнительно принимать значения +inf (положительная бесконечность), -inf (отрицательная бесконечность) и NaN (Not a Number – не число)

Обозначения, которые будут использоваться для описания семантики инструкций сравнения

- I и J – целые числа со знаком, причем I < J
- K и L – целые числа без знака, причем K < L
- A и B – конечные числа с плавающей запятой (то есть они не равны NaN, +inf и -inf), причем A < B
- C – любое число с плавающей запятой (может принимать значения NaN, +inf и -inf)

Инструкция ceq

Код	Инструкция	Встроенный операнд	Описание

0xFE 0x01	**ceq**	–	Сравнение на равенство.
			Для целых чисел:
			`I ceq I => 1,`
			иначе => 0.
			Для чисел с плавающей запятой:
			`+inf ceq +inf => 1,`
			`-inf ceq -inf => 1,`
			`A ceq A => 1,`
			иначе => 0.

Инструкция cgt

Код	Инструкция	Встроенный операнд	Описание

0xFE 0x02	**cgt**	–	Сравнение на "больше".
			Для целых чисел:
			`J cgt I => 1,`
			иначе `=> 0.`
			Для чисел с плавающей запятой:
			`A cgt -inf => 1,`
			`+inf cgt A => 1,`
			`+inf cgt -inf => 1,`
			`B cgt A => 1,`
			иначе `=> 0.`

Инструкция clt

Код	Инструкция	Встроенный операнд	Описание

0xFE 0x04	**clt**	–	Сравнение на "меньше".
			Для целых чисел:
			`I clt J => 1,`
			иначе => 0.
			Для чисел с плавающей запятой:
			`A clt +inf => 1,`
			`-inf clt A => 1,`
			`-inf clt +inf => 1,`
			`A clt B => 1,`
			иначе => 0.

Инструкция cgt.un

Код	Инструкция	Встроенный операнд	Описание

0xFE 0x03	**cgt.**un	–	Сравнение на "больше" беззнаковых целых чисел или неупорядоченных чисел с плавающей запятой.
			Для целых чисел:
			`L cgt.un K => 1,`
			`иначе => 0.`
			Для чисел с плавающей запятой:
			`NaN cgt.un C => 1,`
			`C cgt.un NaN => 1,`
			`A cgt.un -inf => 1,`
			`+inf cgt.un A => 1,`
			`+inf cgt.un -inf => 1,`
			`B cgt.un A => 1,`
			`иначе => 0.`

Инструкция clt.un

Код	Инструкция	Встроенный операнд	Описание

0xFE 0x05	**clt.**un	–	Сравнение на "меньше" беззнаковых целых чисел или неупорядоченных чисел с плавающей запятой.
			Для целых чисел:
			`K clt.un L => 1,`
			иначе => 0.
			Для чисел с плавающей запятой:
			`NaN clt.un C => 1,`
			`C clt.un NaN => 1,`
			`A clt.un +inf => 1,`
			`-inf clt.un A => 1,`
			`-inf clt.un +inf => 1,`
			`A clt.un B => 1,`
			иначе => 0.

9.2.2. Унарные арифметические операции

Код	Инструкция	Встроенный операнд	Описание
0x65	**`neg`**	–	Изменение знака числа
0x66	**`not`**	–	Побитовое НЕ

9.2.3. Инструкция ckfinite

- Инструкция **ckfinite** генерирует исключение ArithmeticException, если число с плавающей запятой, находящееся на вершине стека вычисление, равно NaN, +inf или -inf.

Код	Инструкция	Встроенный операнд	Описание
0xC3	**`ckfinite`**	–	Проверка того, что число с плавающей запятой является конечным

Преобразование значений без контроля переполнения

Код	Инструкция	Встроенный операнд	Описание
0x67	**conv.**i1	–	Преобразовать к int8
0x68	**conv.**i2	–	Преобразовать к int16
0x69	**conv.**i4	–	Преобразовать к int32
0x6A	**conv.**i8	–	Преобразовать к int64
0x6B	**conv.**r4	–	Преобразовать к float32
0x6C	**conv.**r8	–	Преобразовать к float64
0x6D	**conv.**u4	–	Преобразовать к unsigned int32
0x6E	**conv.**u8	–	Преобразовать к unsigned int64
0x76	**conv.**r.un	–	Преобразовать беззнаковое целое число в число с плавающей запятой
0xD1	**conv.**u2	–	Преобразовать к unsigned int16
0xD2	**conv.**u1	–	Преобразовать к unsigned int8
0xD3	**conv.**i	–	Преобразовать к native int
0xE0	**conv.**u	–	Преобразовать к unsigned native int

Преобразование значений со знаком с контролем переполнения

Код	Инструкция	Встроенный операнд	Описание
0xB3	**conv**.ovf.i1	–	Преобразование к int8
0xB4	**conv**.ovf.u1	–	Преобразование к unsigned int8
0xB5	**conv**.ovf.i2	–	Преобразование к int16
0xB6	**conv**.ovf.u2	–	Преобразование к unsigned int16
0xB7	**conv**.ovf.i4	–	Преобразование к int32
0xB8	**conv**.ovf.u4	–	Преобразование к unsigned int32
0xB9	**conv**.ovf.i8	–	Преобразование к int64
0xBA	**conv**.ovf.u8	–	Преобразование к unsigned int64
0xD4	**conv**.ovf.i	–	Преобразование к native int
0xD5	**conv**.ovf.u	–	Преобразование к unsigned native int

Преобразование беззнаковых значений с контролем переполнения

Код	Инструкция	Встроенный операнд	Описание
0x82	**conv**.ovf.i1.un	–	Преобразование к int8
0x83	**conv**.ovf.i2.un	–	Преобразование к int16
0x84	**conv**.ovf.i4.un	–	Преобразование к int32
0x85	**conv**.ovf.i8.un	–	Преобразование к int64
0x86	**conv**.ovf.u1.un	–	Преобразование к unsigned int8
0x87	**conv**.ovf.u2.un	–	Преобразование к unsigned int16
0x88	**conv**.ovf.u4.un	–	Преобразование к unsigned int32
0x89	**conv**.ovf.u8.un	–	Преобразование к unsigned int64
0x8A	**conv**.ovf.i.un	–	Преобразование к native int
0x8B	**conv**.ovf.u.un	–	Преобразование к unsigned native int

9.3. Инструкции для организации передачи управления

- Категории инструкций для передачи управления:
  - Инструкции безусловного перехода
  - Инструкции условного перехода
  - Инструкция switch
  - Инструкция call
  - Инструкция ret

9.3.1. Безусловный переход

Код	Инструкция	Встроенный операнд	Описание
0x2B	**`br.s`**	int8	Короткий безусловный переход
0x38	**`br`**	int32	Длинный безусловный переход

- Диаграмма стека:

  … **`->`** …

Базовые инструкции условного перехода

Код	Инструкция	Встроенный операнд	Описание
0x2C	**`brfalse.`**`s`	int8	Короткий условный переход, если значение равно 0 или null
0x2D	**`brtrue.`**`s`	int8	Короткий условный переход, если значение не равно 0 или null
0x39	**`brfalse`**	int32	Длинный условный переход, если значение равно 0 или null
0x3A	**`brtrue`**	int32	Длинный условный переход, если значение не равно 0 или null

- Диаграмма стека:

  … **`, value ->`** …

Дополнительные длинные инструкции условного перехода

Код	Инструкция	Встроенный операнд	Описание
0x3B	**beq**	int32	**ceq; brtrue**
0x3C	**bge**	int32	*(int)*: **clt; brfalse** *(F)*: **clt.un; brfalse**
0x3D	**bgt**	int32	**cgt; brtrue**
0x3E	**ble**	int32	*(int)*: **cgt; brfalse** *(F)*: **cgt.un; brfalse**
0x3F	**blt**	int32	**clt; brtrue**
0x40	**bne.un**	int32	**ceq; brfalse**
0x41	**bge.un**	int32	*(int)*: **clt.un; brfalse** *(F)*: **clt; brfalse**
0x42	**bgt.un**	int32	**cgt.un; brtrue**
0x43	**ble.un**	int32	*(int)*: **cgt.un; brfalse** *(F)*: **cgt; brfalse**
0x44	**blt.un**	int32	**clt.un; brtrue**

- Диаграмма стека: … **, value1, value2 ->** …

Дополнительные короткие инструкции безусловного перехода

Код	Инструкция	Встроенный операнд	Описание
0x2E	**beq.s**	int8	**ceq; brtrue.**s
0x2F	**bge.**s	int8	*(int)*: **clt; brfalse.**s *(F)*: **clt.**un**; brfalse.**s
0x30	**bgt.**s	int8	**cgt; brtrue.**s
0x31	**ble.**s	int8	*(int)*: **cgt; brfalse.**s *(F)*: **cgt.**un**; brfalse.**s
0x32	**blt.**s	int8	**clt; brtrue.**s
0x33	**bne.**un.s	int8	**ceq; brfalse.**s
0x34	**bge.**un.s	int8	*(int)*: **clt.**un**; brfalse.**s *(F)*: **clt; brfalse.**s
0x35	**bgt.**un.s	int8	**cgt.**un**; brtrue.**s
0x36	**ble.**un.s	int8	*(int)*: **cgt.**un**; brfalse.**s *(F)*: **cgt; brfalse.**s
0x37	**blt.**un.s	int8	**clt.**un**; brtrue.**s

- Диаграмма стека: … **, value1, value2 ->** …

9.3.3. Инструкция switch

Код	Инструкция	Встроенный операнд	Описание
0x42	**`switch`**	unsigned int32, int32 ... int32	Осуществляет переход по таблице переходов в соответствии со значением на вершине стека

- Диаграмма стека:

  …, **`value ->`** …

9.3.4. Инструкция call

Код	Инструкция	Встроенный операнд	Описание
0x28	**`call`**	token	Выполняет вызов метода

- Диаграмма стека:

  … **`, [parameters] -> [result]`**

9.3.5. Инструкция ret

Код	Инструкция	Встроенный операнд	Описание
0x2A	**ret**	–	Осуществляет возврат из метода

- Диаграмма стека:

  … , **[value]** -> … , **[value]**