Богатов Р.Н.

Программирование на языке высокого уровня

Лекция 15.
Битовые операции

Кафедра АСОИУ ОмГТУ, 2013

«Логические» vs. «битовые»

- Двоичные логические операции
  - отрицание (¬)
  - конъюнкция (Λ или &)
  - дизъюнкция (V)
  - сложение по модулю два (⊕)

Конъюнкция

a	b	$a \wedge b$
0	0	0
0	1	0
1	0	0
1	1	1

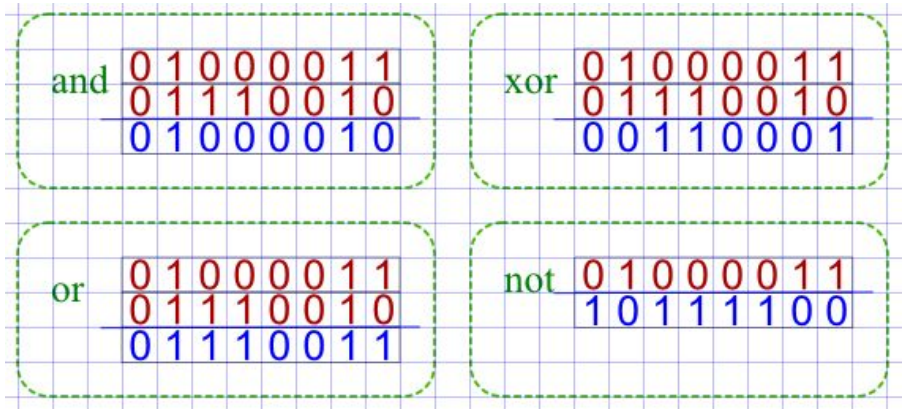
Дизъюнкция

a	b	$a \vee b$
0	0	0
0	1	1
1	0	1
1	1	1

Сложение по модулю 2

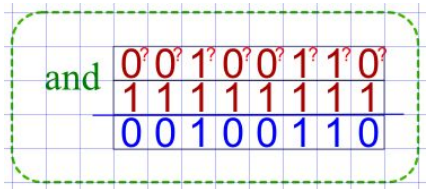
a	b	$a \oplus b$
0	0	0
0	1	1
1	0	1
1	1	0

- Битовые операции
  - побитовое отрицание
  - побитовое И
  - побитовое ИЛИ
  - сложение по модулю два
  - циклический сдвиг

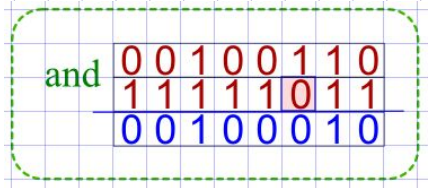


Применение битовых операций

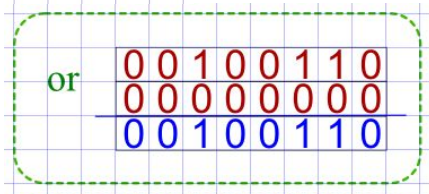
- Проверка битов:

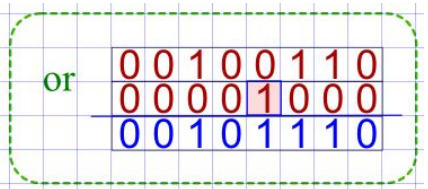


- Обнуление битов:

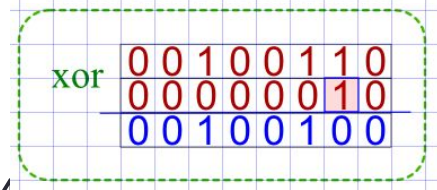


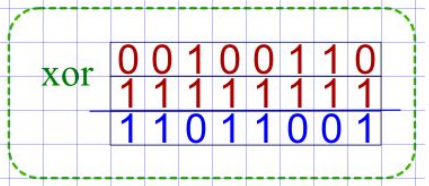
- Установка битов в единицу:



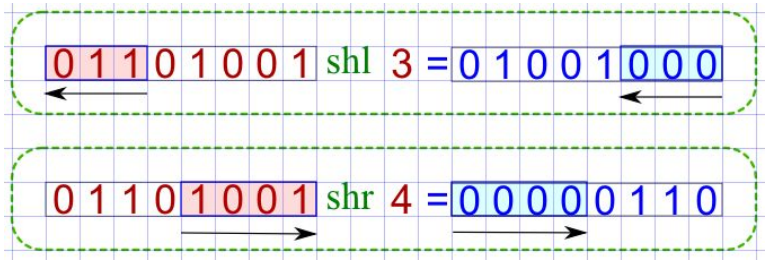


- Смена значений битов:





- Операции побитового циклического сдвига:



Языки программирования

- Логические операции

Язык	НЕ	И	ИЛИ	Искл. ИЛИ	Эквив.	Не экв.
C++[2]	!	&&	||	^	==	!=
Pascal[5]	not	and	or	xor	=	<>

```
if (a != 0 && b/a > 3)
{
    ...
}
```

- Побитовые операции

Язык	НЕ	И	ИЛИ	Искл. ИЛИ	Сдвиг влево	Сдвиг вправо
C/C++, Java, C#, Ruby[4]	~	&	|	^	<<	>>
Pascal[5]	not	and	or	xor	shl	shr

Побитовые чудеса…

```
// Подсчёт ненулевых
uint CountBits(uint x
{
    uint c = 0;
    for (; x != 0; x
        c += x & 1;

    return c;
}
```

```
// Подсчёт ненулевых
uint CountBits(uint x
{
    uint c = 0;
    for (; x != 0; c
        x &= x - 1;
    return c;
}
```

```
// Подсчё
uint Cou
{
    x = x
    x =
    retu
}
```

```
// Вычисление бита чётности
bool ParityBit(uint x)
{
    return (CountBits(x) % 2 != 0);
}
```

```
// Вычисление бита чётности. Оптимизация ;-)
bool ParityBit(uint x)
{
    bool parity = false;
    while (x != 0)
    {
        parity = !parity;
        x = x & (x - 1);
    }
    return parity;
}
```

```
// Вычисление бита чётности. Эммм... 8-/
bool ParityBit(uint x)
{
    x ^= x >> 16;
    x ^= x >> 8;
    x ^= x >> 4;
    x &= 0xf;
    return ((0x6996 >> (int)x) & 1) > 0;
}
```

Больше «чудес»
на странице
bithacks.html
(так её и ищите)

Сложение по модулю 2

eXclusive OR

Свойства

- $a \oplus 0 = a$
- $a \oplus a = 0$
- $a \oplus b = b \oplus a$
- $a \oplus 1 = |\bar{a}|$
- $(a \oplus b) \oplus b = a$
- $\bar{a} \oplus b = a \oplus \bar{b}$

X	Y	Z	⊕(X,Y,Z)
0	0	0	0
1	0	0	1
0	1	0	1
1	1	0	0
0	0	1	1
1	0	1	0
0	1	1	0
1	1	1	1

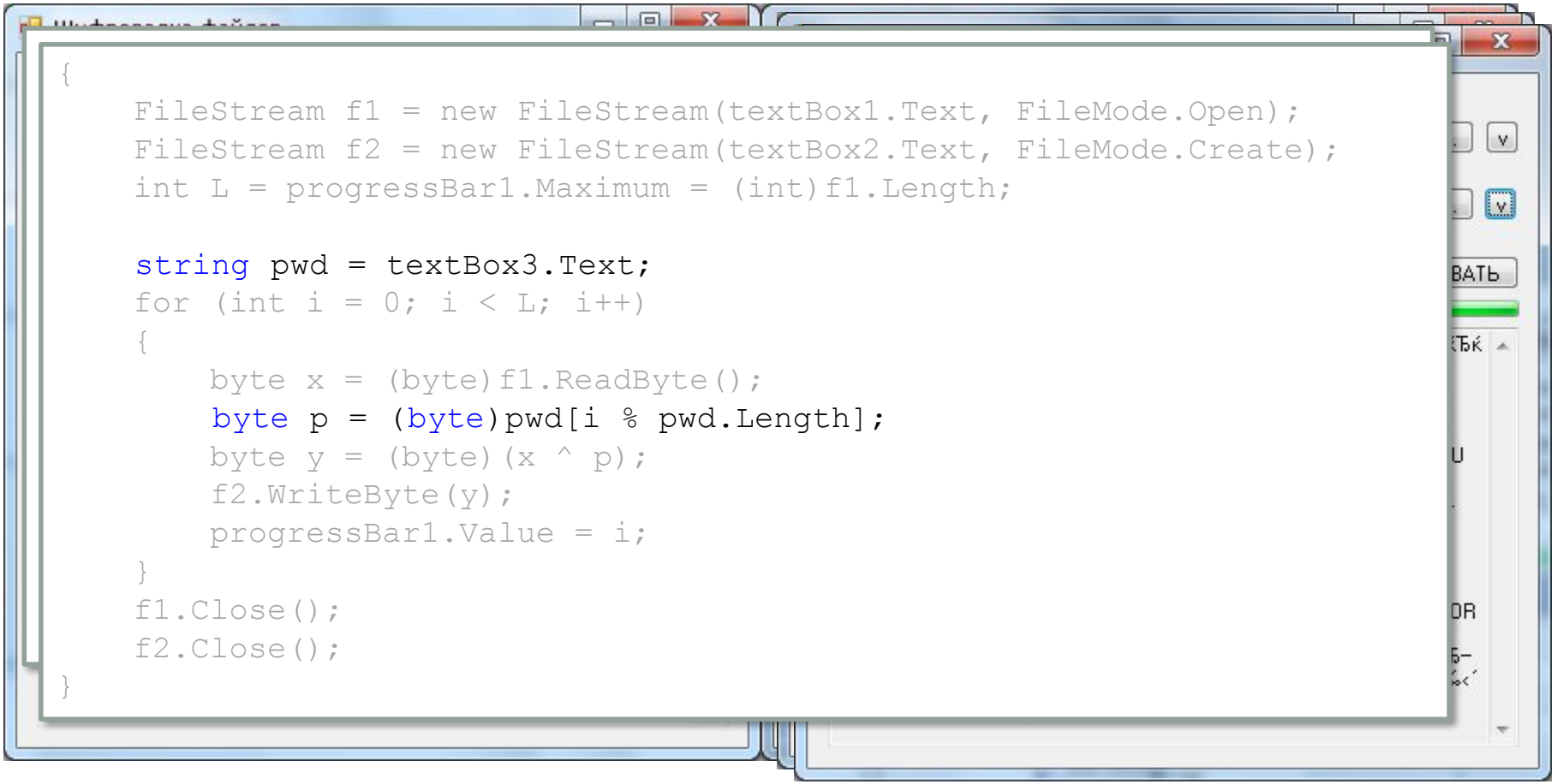
```
// обмен переменных
    ...
    int t = x;
    x = y;
    y = t;
    ...
```

```
// обмен переменных
// без посредника!!!
    ...
    x = x^y;
    y = x^y;
    x = x^y;
    ...
```

Пригождается:

- инверсия по маске
- контроль чётности
- обмен значений переменных
- спрайтовая графика
- криптография

Шифрование файла



```
{
    FileStream f1 = new FileStream(textBox1.Text, FileMode.Open);
    FileStream f2 = new FileStream(textBox2.Text, FileMode.Create);
    int L = progressBar1.Maximum = (int)f1.Length;

    string pwd = textBox3.Text;
    for (int i = 0; i < L; i++)
    {
        byte x = (byte)f1.ReadByte();
        byte p = (byte)pwd[i % pwd.Length];
        byte y = (byte)(x ^ p);
        f2.WriteByte(y);
        progressBar1.Value = i;
    }
    f1.Close();
    f2.Close();
}
```