Subject: Re: random functions proposal
Posted by Sender Ghost on Tue, 17 Jan 2012 19:08:14 GMT
View Forum Message <> Reply to Message

dolik.rce wrote on Tue, 17 January 2012 18:45This pseudo scientific paper seems to propose reasonably simple algorithm that overcomes the obvious problems of the implementation Sender Ghost proposed.

Well, what I "proposed" (and I didn't propose, but just showed a simple solution) is useful for float numbers, not double, hence this Randomf, instead of Randomd, I think.
With qword Random64(qword n) it will be possible to do the same, of course.

mirek wrote on Tue, 17 January 2012 14:24...but it looks like int64 -> double conversion is CPU opcode, so perhaps Random64(int n) as prerequisite, than Randomf() is a good path...
According to "Random number generators discussion" it is possible to combine two random dword values (MAKEQWORD macro might be useful here) to get random qword value.

```
qword Random64()
{
 return MAKEQWORD(Random(), Random());
}

qword Random64(qword n)
{
 qword mask = n, r;
 mask |= mask >> 1; mask |= mask >> 2;
 mask |= mask >> 4; mask |= mask >> 8;
 mask |= mask >> 16; mask |= mask >> 32;

 do
  r = Random64() & mask;
 while(r >= n);
 return r;
}

qword Random64(qword a, qword b)
{
 if (a == b)
  return a;
 if (a < b)
  return a + Random64(b - a + 1);
 return b + Random64(a - b + 1);
}
```

Edit: Added possible Random64 implementation(s).