Binary Polynomial Multiplication Re-re-revisited

Magnus Find, Rene Peralta

Human Nature

Since the dawn of mankind:

How do I do stuff fast?

Hunt, reproduce, eat, sleep, code, drink

Multiplication of binary polynomials

Poly-mult

$$a(x)=a_0+a_1x+a_2x^2+...+a_nx^n$$

$$b(x)=b_0+b_1x+b_2x^2+...+b_nx^n$$

Finite fields of char. 2
elliptic curve crypto, ...

Product

$$c(x)=c_0+c_1x+c_2x^2+...+c_{2n}x^{2n}$$

Where

$$\sum_{i+j=k} a_i b_j \quad \text{Mod 2}$$

Crypto 2009

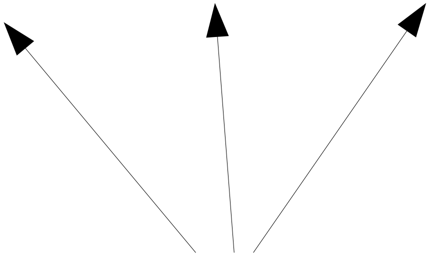
- Dan Bernstein:
  - Recursive constructions
    - (Karatsuba, Toom, Cook)
  - Heuristic postoptimizations
  - Really good values. Improvements??

General Lesson from Karatsuba-type techniques

$$a_0 + a_1 x + ... + a_{n-1} x^{2n} = A_0 + A_1 x^n$$

$$b_0 + b_1 x + ... + b_{n-1} x^{2n} = B_0 + B_1 x^n$$

$A_0 * B_0$ $\quad A_1 * B_1$ $\quad (A_0 + A_1) * (B_0 + B_1)$ $\qquad T(2n) \leqslant 3T(n) + cn$

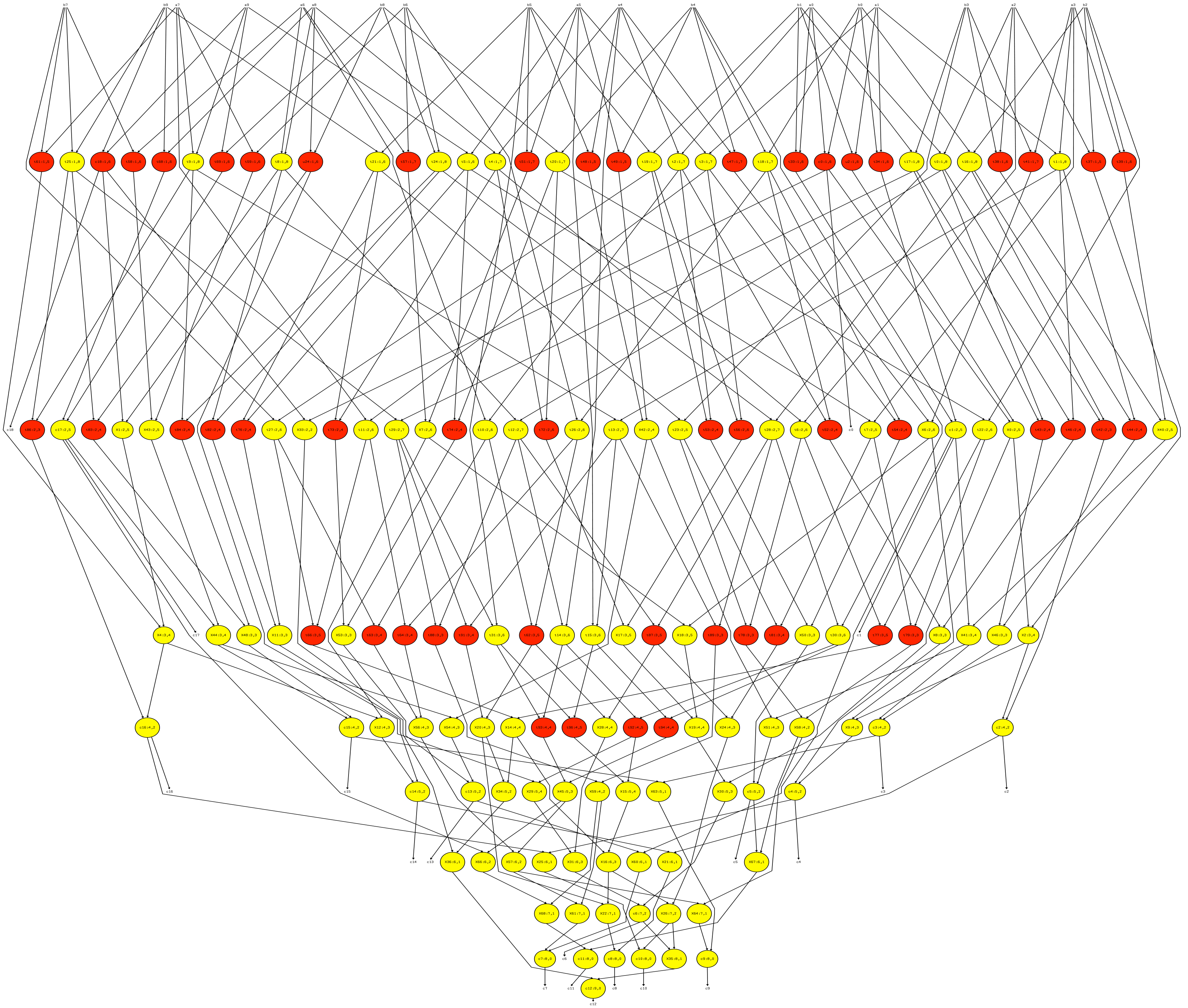


Mult. of degree 1 poly
With 3 multiplications

- *Any* circuit for poly mult gives rise to *<u>some</u>* recurrence relation
- A circuit with **few multiplications** gives better recurrence (maybe)\
-

Multiplicative complexity

Strategy: Use **computer search** to find circuits with **few AND gates**, then use this as recurrence.


b7
b9
a7
a9
a6
a8
b8
b6
b5
a5
a4
b4
b1
a0
b0
a1
b3
a2
a3
b2
t61:1,5
t25:1,8
c18:1,6
t58:1,6
t68:1,6
t9:1,8
t69:1,6
t59:1,6
t8:1,8
u24:1,6
t21:1,6
t57:1,7
t24:1,8
t5:1,6
t4:1,7
t51:1,7
t20:1,7
t48:1,5
t49:1,5
t19:1,7
t2:1,7
t3:1,7
t47:1,7
t18:1,7
t33:1,6
c0:1,6
u2:1,6
t34:1,6
t17:1,8
t0:1,8
t16:1,8
t38:1,6
t41:1,7
t1:1,8
t37:1,5
t39:1,6
c18
t86:2,3
c17:2,5
t83:2,4
X1:2,5
X43:2,5
t84:2,4
t82:2,4
t76:2,4
t27:2,6
X33:2,2
t73:2,4
t11:2,6
t29:2,7
X7:2,6
t74:2,4
t10:2,6
t12:2,7
t72:2,6
t26:2,6
t13:2,7
X42:2,4
t23:2,5
t53:2,4
t56:2,6
t28:2,7
t6:2,6
t52:2,4
c0
t7:2,5
t54:2,4
X6:2,6
c1:2,5
t22:2,6
X0:2,5
t43:2,4
t46:2,4
t42:2,3
t44:2,4
X40:2,5
X4:3,4
c17
X44:3,4
X48:3,3
X11:3,3
t66:3,5
X53:3,3
t63:3,4
t64:3,4
t88:3,3
t91:3,4
t31:3,6
t62:3,5
t14:3,6
t15:3,6
X17:3,5
t87:3,5
X18:3,5
t89:3,3
t78:3,3
t81:3,4
X50:3,3
t30:3,6
c1
t77:3,5
t79:3,3
X8:3,3
X41:3,4
X46:3,3
X2:3,4
c16:4,2
c15:4,2
X12:4,3
X56:4,3
X54:4,3
X20:4,3
X14:4,4
t93:4,4
t96:4,5
X28:4,4
t92:4,5
t94:4,4
X19:4,4
X24:4,3
X51:4,3
X58:4,2
X9:4,3
c3:4,2
c2:4,2
c16
c15
c14:5,2
c13:5,2
X34:5,2
X29:5,4
X45:5,3
X59:4,2
X15:5,4
X63:5,1
X30:5,3
c5:5,2
c4:5,2
c3
c2
c14
c13
X36:6,1
X66:6,2
X57:6,2
X25:6,1
X31:6,3
X16:6,3
X60:6,1
X21:6,1
c5
X67:6,1
c4
X68:7,1
X61:7,1
X22:7,1
c6:7,2
X26:7,2
X64:7,1
c7:8,0
c6
c11:8,0
c8:8,0
c10:8,0
X35:8,1
c9:8,0
c7
c11
c12:9,0
c8
c10
c9
c12

Results

- For 10-bit mult.
- new circuit with 154 gates
- Best had 155
- 1 gate less, but **20** and gates less
- Improvements also for 15-bits and other values

Lesson

- In this day and age there is still room for improvement on how to multiply **very small** polynomials

THANKS