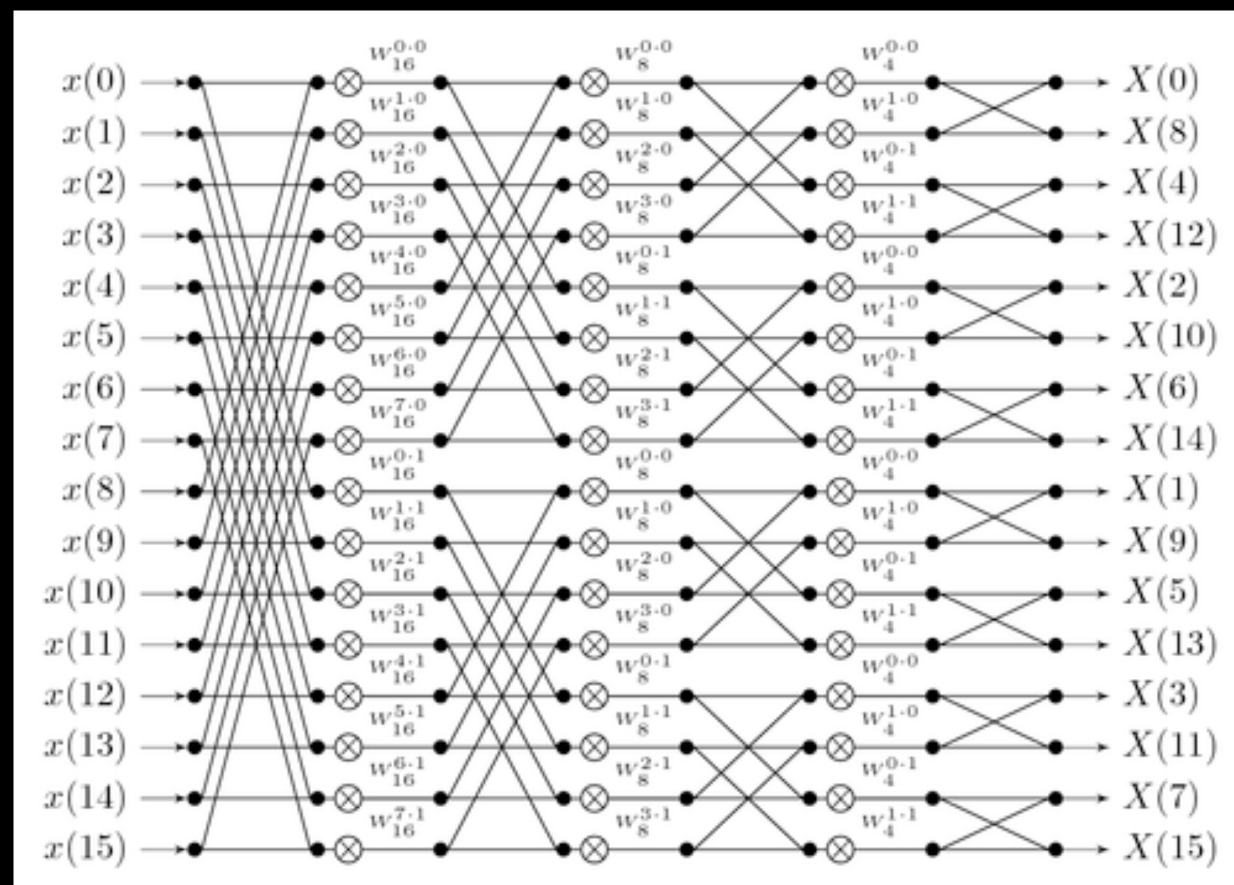
The Complexity of Multiplication in Finite Fields



Amin Shokrollahi
EPFL

$$\mathbb{F}_{p^n}$$

$$\mathbb{F}_{p^n}/\mathbb{F}_p$$

Algorithm

Fast Algorithm

$$a(x)b(x)$$

$$(a_1x + a_0)(b_1x + b_0)$$

$$(a_1x + a_0)(b_1x + b_0)$$

$$(a_1x + a_0)(b_1x + b_0)$$

$$\|$$

$$(a_1 x + a_0)(b_1 x + b_0)$$

$$\|$$

$$a_1 \cdot b_1 \quad x^2$$

$$+$$

$$a_1 \cdot b_0 \quad x$$

$$+$$

$$a_0 \cdot b_1 \quad x$$

$$+$$

$$a_0 \cdot b_0 \quad 1$$

$$
\begin{array}{ccc}
a_1 \cdot b_1 & & x^2 \\
+ & & \\
a_1 \cdot b_0 & & x \\
+ & & \\
a_0 \cdot b_1 & & x \\
+ & & \\
a_0 \cdot b_0 & & 1
\end{array}
\quad = \quad
\begin{array}{ccc}
f_1(a) \cdot g_1(b) & & w_1 \\
+ & & \\
f_2(a) \cdot g_2(b) & & w_2 \\
+ & & \\
f_3(a) \cdot g_3(b) & & w_3 \\
+ & & \\
f_4(a) \cdot g_4(b) & & w_4
\end{array}
$$

$$U, V, W$$

U, V, W Finite dimensional spaces over $\mathbb{F}$

U, V, W Finite dimensional spaces over $\mathbb{F}$

$$\phi\colon U \times V \to W$$

U, V, W Finite dimensional spaces over $\mathbb{F}$

$\phi\colon U \times V \longrightarrow W$ Bilinear map

U, V, W Finite dimensional spaces over $\mathbb{F}$

$\phi \colon U \times V \to W$ Bilinear map

U, V, W Finite dimensional spaces over $\mathbb{F}$

$\phi\colon U \times V \longrightarrow W$ Bilinear map

$$f_1, \ldots, f_r \in U^*$$

$$g_1, \ldots, g_r \in V^*$$

$$w_1, \ldots, w_r \in W$$

U, V, W Finite dimensional spaces over $\mathbb{F}$

$\phi\colon U \times V \to W$ Bilinear map

$f_1, \ldots, f_r \in U^*$

$g_1, \ldots, g_r \in V^*$ Bilinear algorithm for ϕ

$w_1, \ldots, w_r \in W$

Bilinear algorithm for ϕ

$$f_1, \ldots, f_r \in U^*$$

$$g_1, \ldots, g_r \in V^*$$

$$w_1, \ldots, w_r \in W$$

$$\forall a \in U, b \in V: \qquad \phi(a, b) = \sum_{i=1}^{r} f_i(a) g_i(b) w_i$$

Bilinear algorithm for ϕ

$$f_1, \ldots, f_r \in U^*$$

$$g_1, \ldots, g_r \in V^*$$

$$w_1, \ldots, w_r \in W$$

$$\forall a \in U, b \in V: \qquad \phi(a,b) = \sum_{i=1}^{r} f_i(a) g_i(b) w_i$$

r = Length of the algorithm

Bilinear algorithm for ϕ

$$f_1, \ldots, f_r \in U^*$$

$$g_1, \ldots, g_r \in V^*$$

$$w_1, \ldots, w_r \in W$$

$$\forall a \in U, b \in V: \qquad \phi(a,b) = \sum_{i=1}^{r} f_i(a) g_i(b) w_i$$

r = Length of the algorithm

$R(\phi)$ = minimum such r

Rank (bilinear complexity) of ϕ

Quadratic algorithm for ϕ

Quadratic algorithm for ϕ

$$f_1, \ldots, f_r \in (U \times V)^*$$
$$g_1, \ldots, g_r \in (U \times V)^*$$
$$w_1, \ldots, w_r \in w$$

Quadratic algorithm for ϕ

$$f_1, \ldots, f_r \in (U \times V)^*$$
$$g_1, \ldots, g_r \in (U \times V)^*$$
$$w_1, \ldots, w_r \in w$$

$$\forall a \in U, b \in V: \qquad \phi(a,b) = \sum_{i=1}^{r} f_i(a,b) g_i(a,b) w_i$$

Quadratic algorithm for ϕ

$$f_1, \ldots, f_r \in (U \times V)^*$$
$$g_1, \ldots, g_r \in (U \times V)^*$$
$$w_1, \ldots, w_r \in w$$

$$\forall a \in U, b \in V: \quad \phi(a,b) = \sum_{i=1}^{r} f_i(a,b) g_i(a,b) w_i$$

r = Length of the algorithm

Quadratic algorithm for ϕ

$$f_1, \ldots, f_r \in (U \times V)^*$$
$$g_1, \ldots, g_r \in (U \times V)^*$$
$$w_1, \ldots, w_r \in w$$

$$\forall a \in U, b \in V: \qquad \phi(a,b) = \sum_{i=1}^{r} f_i(a,b) g_i(a,b) w_i$$

r = Length of the algorithm

$L(\phi)$ = minimum such r

Quadratic complexity of ϕ

$$\frac{1}{2}R(\phi) \leq L(\phi) \leq R(\phi)$$

Volker Strassen
1970

Volker Strassen
1970

Volker Strassen
1970

Over an infinite field quadratic complexity is the right measure (no divisions needed).

Why rank?

Well behaved

$$\phi\colon U \times V \longrightarrow W$$

$$\phi\colon U \times V \longrightarrow W$$

$$\phi'\colon U' \times V' \longrightarrow W'$$

$\phi\colon U \times V \longrightarrow W$

$\phi'\colon U' \times V' \rightarrow W'$

$$\phi : U \times V \longrightarrow W \qquad \phi' : U' \times V' \longrightarrow W'$$

$$\phi \oplus \phi' : U \oplus U' \times V \oplus V' \longrightarrow W \oplus W'$$

$$\phi\colon U \times V \to W \qquad\qquad \phi'\colon U' \times V' \to W'$$

$$\phi \oplus \phi'\colon U \oplus U' \times V \oplus V' \to W \oplus W'$$

$$\phi \otimes \phi'\colon U \otimes U' \times V \otimes V' \to W \otimes W'$$

$$\phi : U \times V \longrightarrow W \qquad \phi' : U' \times V' \longrightarrow W'$$

$$\phi \oplus \phi' : U \oplus U' \times V \oplus V' \longrightarrow W \oplus W'$$

$$\phi \otimes \phi' : U \otimes U' \times V \otimes V' \longrightarrow W \otimes W'$$

$$\phi \colon U \times V \to W \qquad \phi' \colon U' \times V' \to W'$$

$$\phi \oplus \phi' \colon U \oplus U' \times V \oplus V' \to W \oplus W'$$

$$\phi \otimes \phi' \colon U \otimes U' \times V \otimes V' \to W \otimes W'$$

$$R(\phi \oplus \phi') \leq R(\phi) + R(\phi') \qquad L(\phi \oplus \phi') \leq L(\phi) + L(\phi')$$

$$\phi\colon U \times V \longrightarrow W \qquad \phi'\colon U' \times V' \longrightarrow W'$$

$$\phi \oplus \phi'\colon U \oplus U' \times V \oplus V' \longrightarrow W \oplus W'$$

$$\phi \otimes \phi'\colon U \otimes U' \times V \otimes V' \longrightarrow W \otimes W'$$

$$R(\phi \oplus \phi') \leq R(\phi) + R(\phi') \qquad L(\phi \oplus \phi') \leq L(\phi) + L(\phi')$$

$$R(\phi \otimes \phi') \leq R(\phi)R(\phi')$$

$$\phi : U \times V \to W \qquad \phi' : U' \times V' \to W'$$

$$\phi \oplus \phi' : U \oplus U' \times V \oplus V' \to W \oplus W'$$

$$\phi \otimes \phi' : U \otimes U' \times V \otimes V' \to W \otimes W'$$

$$R(\phi \oplus \phi') \leq R(\phi) + R(\phi') \qquad L(\phi \oplus \phi') \leq L(\phi) + L(\phi')$$

$$R(\phi \otimes \phi') \leq R(\phi)R(\phi') \qquad L(\phi \otimes \phi') \not\leq L(\phi)L(\phi')$$

$$\Pi_n : \quad \mathbb{F}_{p^n} \times \mathbb{F}_{p^n} \longrightarrow \mathbb{F}_{p^n}$$

$$F_n := R(\Pi_n)$$

$\Pi_n : \quad \mathbb{F}_{p^n} \times \mathbb{F}_{p^n} \longrightarrow \mathbb{F}_{p^n}$ $\qquad F_n := R(\Pi_n)$

$$F_n := R(\Pi_n)$$

$$F_n := R(\Pi_n)$$

Exact values

$$F_n := R(\Pi_n)$$

Exact values

Asymptotic values

$$\Phi_{k,m}: \quad \mathbb{F}_p[x]_{<k} \times \mathbb{F}_p[x]_{<m} \to \mathbb{F}_p[x]_{<m+k-1}$$

$$P_{k,m} := R(\Phi_{k,m})$$

Simulation Lemma

Simulation Lemma

$$U \times V \xrightarrow{\phi} W$$

Simulation Lemma

$$U \times V \xrightarrow{\phi} W$$

$$U' \times V' \xrightarrow{\phi'} W'$$

Simulation Lemma

$$\begin{tikzcd} U \times V \arrow[r, "\phi"] \arrow[d, "\alpha"', shift right=6ex] \arrow[d, "\beta", shift left=2ex] & W \\ U' \times V' \arrow[r, "\phi'"] & W' \end{tikzcd}$$

Simulation Lemma

$$\begin{tikzcd}
U \times V \arrow[r, "\phi"] \arrow[d, "\alpha"'] & W \\
U' \times V' \arrow[r, "\phi'"] & W' \arrow[u, "\gamma"']
\end{tikzcd}$$

$$U \xrightarrow{\alpha} U', \quad V \xrightarrow{\beta} V'$$

Simulation Lemma

$$\begin{tikzcd} U \times V \arrow[r, "\phi"] \arrow[d, "\alpha"'] & W \\ U' \times V' \arrow[r, "\phi'"] & W' \arrow[u, "\gamma"'] \end{tikzcd}$$

$$\beta : V \to V'$$

ϕ can be simulated by ϕ'

$$R(\phi) \leq R(\phi')$$

$$
\begin{tikzcd}
U \times V \arrow[r, "\phi"] \arrow[d, "\alpha"'] & W \\
U' \times V' \arrow[r, "\phi'"] & W' \arrow[u, "\gamma"']
\end{tikzcd}
$$

$$\begin{tikzcd}
\mathbb{F}_{p^n} \times \mathbb{F}_{p^n} \arrow[rr, "\Pi_n"] \arrow[d, "\alpha"'] \arrow[d, shift left=20, "\beta"] & & \mathbb{F}_{p^n} \\
U' \times V' \arrow[rr, "\phi'"] & & W' \arrow[u, "\gamma"']
\end{tikzcd}$$

$$
\begin{tikzcd}
\mathbb{F}_{p^n} \times \mathbb{F}_{p^n} \arrow[r, "\Pi_n"] \arrow[d, "\alpha"', "\beta"] & \mathbb{F}_{p^n} \\
\mathbb{F}_p[x]_{<n} \times \mathbb{F}_p[x]_{<n} \arrow[r, "\Phi_{n,n}"'] & \mathbb{F}_p[x]_{<2n-1} \arrow[u, "\gamma"']
\end{tikzcd}
$$

$$\begin{tikzcd}
\mathbb{F}_{p^n} \times \mathbb{F}_{p^n} \arrow[r, "\Pi_n"] \arrow[d, "\mathrm{id}"' , "\mathrm{id}"] & \mathbb{F}_{p^n} \\
\mathbb{F}_p[x]_{<n} \times \mathbb{F}_p[x]_{<n} \arrow[r, "\Phi_{n,n}"'] & \mathbb{F}_p[x]_{<2n-1} \arrow[u, "\mathrm{mod}"']
\end{tikzcd}$$

$$
\begin{tikzcd}
\mathbb{F}_{p^n} \times \mathbb{F}_{p^n} \arrow[r, "\Pi_n"] \arrow[d, "\mathrm{id}"'] & \mathbb{F}_{p^n} \\
\mathbb{F}_p[x]_{<n} \times \mathbb{F}_p[x]_{<n} \arrow[r, "\Phi_{n,n}"'] & \mathbb{F}_p[x]_{<2n-1} \arrow[u, "\mathrm{mod}"']
\end{tikzcd}
$$

$$\begin{tikzcd}
\mathbb{F}_{p^n} \arrow[d, "\mathrm{id}"'] & \times & \mathbb{F}_{p^n} \arrow[d, "\mathrm{id}"] \arrow[r, "\Pi_n"] & \mathbb{F}_{p^n} \\
\mathbb{F}_p[x]_{<n} & \times & \mathbb{F}_p[x]_{<n} \arrow[r, "\Phi_{n,n}"'] & \mathbb{F}_p[x]_{<2n-1} \arrow[u, "\mathrm{mod}"']
\end{tikzcd}$$

$$\begin{tikzcd} \mathbb{F}_{p^n} \times \mathbb{F}_{p^n} \arrow[r, "\Pi_n"] \arrow[d, "\mathrm{id}"'] & \mathbb{F}_{p^n} \\ \mathbb{F}_p[x]_{<n} \times \mathbb{F}_p[x]_{<n} \arrow[r, "\Phi_{n,n}"'] & \mathbb{F}_p[x]_{<2n-1} \arrow[u, "\mathrm{mod}"'] \end{tikzcd}$$

$$R(\Pi_n) \leq R(\Phi_{n,n})$$

$$F_n \leq P_{n,n}$$

Naive polynomial multiplication

$$P_{n,n} \leq n^2$$

Naive polynomial multiplication

$$F_n \leq P_{n,n} \leq n^2$$

$$F_n \leq ?$$

$$F_n \leq ?$$

n	naive
1	1
2	4
3	9
4	16
5	25
6	36
7	49
8	64
9	81
10	100

Anatolii Alexeevich
Karatsuba

Anatolii Alexeevich
Karatsuba

$$P_{2,2} \leq 3$$

A. Karatsuba + Y. Ofman

$$(a_1x + a_0)(b_1x + b_0)$$

$$(a_1 x + a_0)(b_1 x + b_0)$$

$$\|$$

$$a_0 \cdot b_0 (1 - x)$$

$$+$$

$$(a_0 + a_1) \cdot (b_0 + b_1) x$$

$$+$$

$$a_1 \cdot b_1 (x^2 - x)$$

$$F_n \leq ?$$

n	naive
1	1
2	4
3	9
4	16
5	25
6	36
7	49
8	64
9	81
10	100

$$F_n \leq ?$$

n	naive	K-O
1	1	1
2	4	3
3	9	
4	16	
5	25	
6	36	
7	49	
8	64	
9	81	
10	100	

Simulation lemma

Simulation lemma

$$(m, n) \leq (m', n') \implies P_{m,n} \leq P_{m',n'}$$

$$(m, n) \leq (m', n') \implies P_{m,n} \leq P_{m',n'}$$

$$(m,n) \leq (m',n') \implies P_{m,n} \leq P_{m',n'}$$

$$\Phi_{m,n} \otimes \Phi_{m',n'} \simeq \Phi_{mm',nn'}$$

$$(m,n) \le (m',n') \implies P_{m,n} \le P_{m',n'}$$

$$P_{mm',nn'} \le P_{m,n}P_{m',n'}$$

$$(m,n) \leq (m',n') \implies P_{m,n} \leq P_{m',n'}$$

$$P_{mm',nn'} \leq P_{m,n} P_{m',n'}$$

$$(m,n) \leq (m',n') \implies P_{m,n} \leq P_{m',n'}$$

$$P_{mm',nn'} \leq P_{m,n} P_{m',n'}$$

$$n \leq 2^m \implies F_n \leq 3^m$$

$$F_n \leq ?$$

n	naive	K-O
1	1	1
2	4	3
3	9	
4	16	
5	25	
6	36	
7	49	
8	64	
9	81	
10	100	

$$F_n \leq ?$$

n	naive	K-O
1	1	1
2	4	3
3	9	9
4	16	9
5	25	27
6	36	27
7	49	27
8	64	27
9	81	81
10	100	81

$$F_n \leq ?$$

n	naive	K-O
1	1	1
2	4	3
3	9	7
4	16	9
5	25	27
6	36	27
7	49	27
8	64	27
9	81	81
10	100	81

$$F_n \leq ?$$

n	naive	K-O
1	1	1
2	4	3
3	9	7
4	16	9
5	25	19
6	36	27
7	49	27
8	64	27
9	81	81
10	100	81

$$F_n \leq ?$$

n	naive	K-O
1	1	1
2	4	3
3	9	7
4	16	9
5	25	19
6	36	21
7	49	27
8	64	27
9	81	81
10	100	81

$$F_n \leq ?$$

n	naive	K-O
1	1	1
2	4	3
3	9	7
4	16	9
5	25	19
6	36	21
7	49	27
8	64	27
9	81	55
10	100	81

$$F_n \leq ?$$

n	naive	K-O
1	1	1
2	4	3
3	9	7
4	16	9
5	25	19
6	36	21
7	49	27
8	64	27
9	81	55
10	100	57

$$F_n \leq ?$$

n	naive	K-O
1	1	1
2	4	3
3	9	7
4	16	9
5	25	19
6	36	21
7	49	27
8	64	27
9	81	55
10	100	57

$F_3 \leq 7$

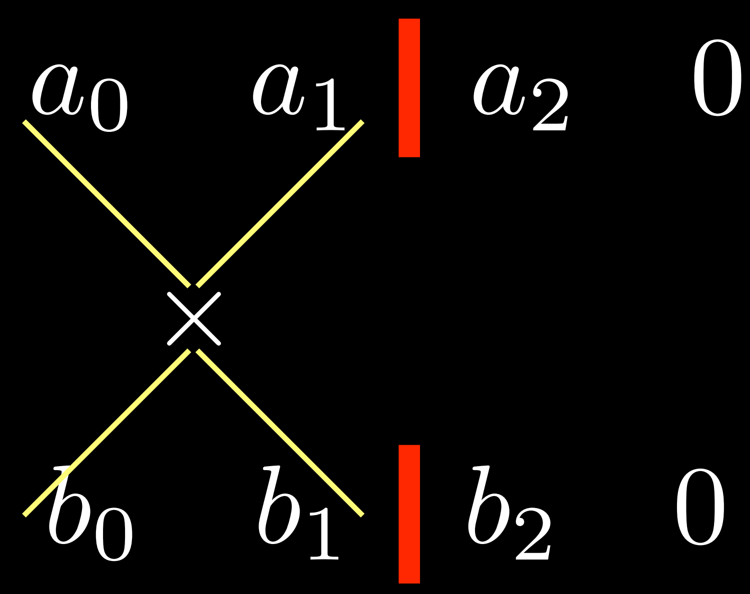
$$\begin{array}{cccc} a_0 & a_1 & a_2 & 0 \\ \\ b_0 & b_1 & b_2 & 0 \end{array}$$

$$F_3 \leq 7$$

$$a_0 \quad a_1 \mid a_2 \quad 0$$

$$b_0 \quad b_1 \mid b_2 \quad 0$$

$$F_3 \le 7$$



$$F_3 \leq 7$$

$$a_0 \quad a_1 \mid a_2 \quad 0$$

$$b_0 \quad b_1 \mid b_2 \quad 0$$

3

$F_3 \leq 7$

$$\begin{tikzcd} a_0 & a_1 & a_2 & 0 \arrow[lll, bend right, "+"'] \end{tikzcd}$$

$$\begin{tikzcd} b_0 & b_1 & b_2 & 0 \arrow[lll, bend left, "+"] \end{tikzcd}$$

3

$F_3 \leq 7$

$$+$$

$$a_0 \quad a_1 \mid a_2 \quad 0$$

$$\times$$

$$b_0 \quad b_1 \mid b_2 \quad 0$$

$$+$$

3

$$F_3 \leq 7$$

$$a_0 \quad a_1 \mid a_2 \quad 0$$

$$b_0 \quad b_1 \mid b_2 \quad 0$$

3 + 3

$F_3 \leq 7$

$a_0 \quad a_1 \;|\; a_2 \quad 0$

$\times$

$b_0 \quad b_1 \;|\; b_2 \quad 0$

3 + 3

$$F_3 \leq 7$$

$$a_0 \quad a_1 \mid a_2 \quad 0$$

$$b_0 \quad b_1 \mid b_2 \quad 0$$

3 + 3 + 1 = 7

$$a(x) = a_0 + a_1 x \qquad b(x) = b_0 + b_1 x$$

$$a(x) = a_0 + a_1 x \qquad b(x) = b_0 + b_1 x$$

$$a_0 \cdot b_0$$

$$(a_0 + a_1) \cdot (b_0 + b_1)$$

$$a_1 \cdot b_1$$

$$a(x) = a_0 + a_1 x \qquad b(x) = b_0 + b_1 x$$

$$a_0 \cdot b_0 \qquad = a(0)b(0)$$

$$(a_0 + a_1) \cdot (b_0 + b_1)$$

$$a_1 \cdot b_1$$

$$a(x) = a_0 + a_1 x \qquad b(x) = b_0 + b_1 x$$

$$a_0 \cdot b_0 \qquad = a(0)b(0)$$

$$(a_0 + a_1) \cdot (b_0 + b_1) \qquad = a(1)b(1)$$

$$a_1 \cdot b_1$$

$$a(x) = a_0 + a_1 x \qquad b(x) = b_0 + b_1 x$$

$$a_0 \cdot b_0 = a(0)b(0)$$

$$(a_0 + a_1) \cdot (b_0 + b_1) = a(1)b(1)$$

$$a_1 \cdot b_1 = a(\infty)b(\infty)$$

Karatsuba-Ofman = Interpolation

Fiduccia and Zalcstein, 1977

$$\Phi_{k,m}: \quad \mathbb{F}_p[x]_{<k} \times \mathbb{F}_p[x]_{<m} \to \mathbb{F}_p[x]_{<m+k-1}$$

Fiducca and Zalcstein, 1977

$$\Phi_{k,m}: \quad \mathbb{F}_p[x]_{<k} \times \mathbb{F}_p[x]_{<m} \to \mathbb{F}_p[x]_{<m+k-1}$$

Need *m*+*k*-1 evaluation points
One can be infinity

Fiduccia and Zalcstein, 1977

$$\Phi_{k,m}: \quad \mathbb{F}_p[x]_{<k} \times \mathbb{F}_p[x]_{<m} \to \mathbb{F}_p[x]_{<m+k-1}$$

$$p \geq m + k - 2 \Longrightarrow P_{k,m} \leq m + k - 1$$

Fiduccia and Zalcstein, 1977

$$\Phi_{k,m} : \quad \mathbb{F}_p[x]_{<k} \times \mathbb{F}_p[x]_{<m} \to \mathbb{F}_p[x]_{<m+k-1}$$

$$p \geq m + k - 2 \implies P_{k,m} \leq m + k - 1$$

$$p \geq 2n - 2 \implies F_n \leq 2n - 1$$

Fiduccia and Zalcstein, 1977

$$F_n \geq 2n - 1$$

Fiduccia and Zalcstein, 1977

$$F_n \geq 2n - 1$$

$$ab = f_1(a)g_1(b)w_1 + f_2(a)g_2(b)w_2 + \cdots + f_r(a)g_r(b)w_r$$

Fiducca and Zalcstein, 1977

$$F_n \geq 2n - 1$$

$$ab = f_1(a)g_1(b)w_1 + f_2(a)g_2(b)w_2 + \cdots + f_r(a)g_r(b)w_r$$

$$\dim\langle f_1, \ldots, f_r \rangle = n$$

Fiduccia and Zalcstein, 1977

$$F_n \geq 2n - 1$$

$$ab = f_1(a)g_1(b)w_1 + f_2(a)g_2(b)w_2 + \cdots + f_r(a)g_r(b)w_r$$

$$\dim\langle f_1, \ldots, f_r \rangle = n$$

Otherwise $a\mathbb{F}_{p^n} = 0$ for some nonzero a

Fiduccia and Zalcstein, 1977

$$F_n \geq 2n - 1$$

$$ab = f_1(a)g_1(b)w_1 + f_2(a)g_2(b)w_2 + \cdots + f_r(a)g_r(b)w_r$$

$$\dim\langle f_1, \ldots, f_r \rangle = n$$

Fiduccia and Zalcstein, 1977

$$F_n \geq 2n - 1$$

$$ab = f_1(a)g_1(b)w_1 + f_2(a)g_2(b)w_2 + \cdots + f_r(a)g_r(b)w_r$$

$$\dim\langle f_1, \ldots, f_r\rangle = n$$

$$0 \neq a \text{ such that} f_1(a) = \cdots = f_{n-1}(a) = 0$$

Fiduccia and Zalcstein, 1977

$$F_n \geq 2n - 1$$

$$ab = f_1(a)g_1(b)w_1 + f_2(a)g_2(b)w_2 + \cdots + f_r(a)g_r(b)w_r$$

$$\dim\langle f_1, \ldots, f_r\rangle = n$$

$$0 \neq a \text{ such that} f_1(a) = \cdots = f_{n-1}(a) = 0$$

$$a\mathbb{F}_{p^n} = f_n(a)g_n(\mathbb{F}_{p^n})w_n + \cdots + f_r(a)g_n(\mathbb{F}_{p^r})w_r$$

Fiduccia and Zalcstein, 1977

$$F_n \geq 2n - 1$$

$$ab = f_1(a)g_1(b)w_1 + f_2(a)g_2(b)w_2 + \cdots + f_r(a)g_r(b)w_r$$

$$\dim\langle f_1, \ldots, f_r\rangle = n$$

$$0 \neq a \text{ such that} f_1(a) = \cdots = f_{n-1}(a) = 0$$

$$a\mathbb{F}_{p^n} = f_n(a)g_n(\mathbb{F}_{p^n})w_n + \cdots + f_r(a)g_n(\mathbb{F}_{p^r})w_r$$

$n = \dim$

Fiducca and Zalcstein, 1977

$$F_n \geq 2n - 1$$

$$ab = f_1(a)g_1(b)w_1 + f_2(a)g_2(b)w_2 + \cdots + f_r(a)g_r(b)w_r$$

$$\dim\langle f_1, \ldots, f_r \rangle = n$$

$$0 \neq a \text{ such that } f_1(a) = \cdots = f_{n-1}(a) = 0$$

$$a\mathbb{F}_{p^n} = f_n(a)g_n(\mathbb{F}_{p^n})w_n + \cdots + f_r(a)g_n(\mathbb{F}_{p^r})w_r$$

$n = \dim$ $\qquad$ $\dim \leq r - n + 1$

Fiduccia and Zalcstein, 1977

$$F_n \geq 2n - 1$$

$$ab = f_1(a)g_1(b)w_1 + f_2(a)g_2(b)w_2 + \cdots + f_r(a)g_r(b)w_r$$

$$\dim\langle f_1, \ldots, f_r\rangle = n$$

$$0 \neq a \text{ such that } f_1(a) = \cdots = f_{n-1}(a) = 0$$

$$a\mathbb{F}_{p^n} = f_n(a)g_n(\mathbb{F}_{p^n})w_n + \cdots + f_r(a)g_n(\mathbb{F}_{p^r})w_r$$

$$n \leq r - n + 1$$

Fiduccia and Zalcstein, 1977

$$F_n \geq 2n - 1$$

$$ab = f_1(a)g_1(b)w_1 + f_2(a)g_2(b)w_2 + \cdots + f_r(a)g_r(b)w_r$$

$$\dim\langle f_1, \ldots, f_r \rangle = n$$

$$0 \neq a \text{ such that} f_1(a) = \cdots = f_{n-1}(a) = 0$$

$$a\mathbb{F}_{p^n} = f_n(a)g_n(\mathbb{F}_{p^n})w_n + \cdots + f_r(a)g_n(\mathbb{F}_{p^r})w_r$$

$$2n - 1 \leq r$$

$$F_n = 2n - 1$$

if

$$p \geq 2n - 2$$

$$F_n = 2n - 1$$

iff

$$p \geq 2n - 2$$

Wingorad, deGroote

Case closed for large fields

n	naive	K-O
1	1	1
2	4	3
3	9	7
4	16	9
5	25	19
6	36	21
7	49	27
8	64	27
9	81	55
10	100	57

n	naive	K-O	LB
1	1	1	1
2	4	3	3
3	9	7	6
4	16	9	8
5	25	19	10
6	36	21	12
7	49	27	14
8	64	27	16
9	81	55	18
10	100	57	20

$p=2$

$$p = 2$$

$$F_n = O\left(n^{\frac{\log(3)}{\log(2)}}\right)$$

$$p = 2$$

$$F_n = O\left(n^{\frac{\log(3)}{\log(2)}}\right)$$

$$p = 2$$

$$F_n = O\left(n^{\frac{\log(3)}{\log(2)}}\right)$$

$$p > 2$$

$$F_n = O\left(n^{\frac{\log(p+1)}{\log(p+1)-\log(2)}}\right)$$

Small base field

$$\mathbb{F}_p[x]_{<n} \quad \times \quad \mathbb{F}_p[x]_{<n} \longrightarrow \mathbb{F}_p[x]_{<2n-1}$$

$$\mathbb{F}_p[x]_{<n}$$

$$\downarrow$$

$$\mathbb{F}_p[x]/(x-\alpha_1) \times \cdots \times \mathbb{F}_p[x]/(x-\alpha_{2n-1})$$

$\alpha_1, \ldots, \alpha_{2n-1}$ pairwise distinct in $\mathbb{F}_p$

$$\mathbb{F}_p[x]/(x-\alpha_1) \times \cdots \times \mathbb{F}_p[x]/(x-\alpha_{2n-1})$$

$$\mathbb{F}_p[x]/(x-\alpha_1) \times \cdots \times \mathbb{F}_p[x]/(x-\alpha_{2n-1})$$

$$\shortparallel$$

$$V_n$$

$$\mathbb{F}_p[x]/(x-\alpha_1) \times \cdots \times \mathbb{F}_p[x]/(x-\alpha_{2n-1})$$

$$\parallel$$

$$V_n$$

$$\mathbb{F}_p[x]_{<n} \quad \times \quad \mathbb{F}_p[x]_{<n} \xrightarrow{\Phi_{n,n}} \mathbb{F}_p[x]_{<2n-1}$$

$$\mathbb{F}_p[x]/(x-\alpha_1) \times \cdots \times \mathbb{F}_p[x]/(x-\alpha_{2n-1})$$

$$\shortparallel$$

$$V_n$$

$$\mathbb{F}_p[x]_{<n} \quad \times \quad \mathbb{F}_p[x]_{<n} \xrightarrow{\Phi_{n,n}} \mathbb{F}_p[x]_{<2n-1}$$

$$V_n \quad \times \quad V_n \longrightarrow V_n$$

$$\mathbb{F}_p[x]/(x-\alpha_1) \times \cdots \times \mathbb{F}_p[x]/(x-\alpha_{2n-1})$$

$$\shortparallel$$

$$V_n$$

$$\mathbb{F}_p[x]_{<n} \quad \times \quad \mathbb{F}_p[x]_{<n} \xrightarrow{\Phi_{n,n}} \mathbb{F}_p[x]_{<2n-1}$$

$$V_n \quad \times \quad V_n \xrightarrow{\Phi_{1,1} \oplus \cdots \oplus \Phi_{1,1}} V_n$$

$$
\begin{tikzcd}
\mathbb{F}_p[x]_{<n} \arrow[d] & \times & \mathbb{F}_p[x]_{<n} \arrow[d] \arrow[r, "\Phi_{n,n}"] & \mathbb{F}_p[x]_{<2n-1} \arrow[d, phantom, "\cong" rotate=-90] \\
V_n & \times & V_n \arrow[r, "\Phi_{1,1} \oplus \cdots \oplus \Phi_{1,1}"] & V_n
\end{tikzcd}
$$

$$R(\Phi_{n,n}) \leq (2n-1)R(\Phi_{1,1}) = 2n - 1$$

$$\mathbb{F}_p[x]_{<2n-1}$$

Chinese remaindering

$$\mathbb{F}_p[x]_{<2n-1}$$

$$\wr\!|\!|$$

$$\mathbb{F}_p[x]/(x-\alpha_1) \times \cdots \times \mathbb{F}_p[x]/(x-\alpha_{2n-1})$$

and “respects” multiplication

Chinese remaindering

$$\mathbb{F}_p[x]_{<2n-1}$$

$$\cong$$

$$\mathbb{F}_p[x]/f_1(x) \times \cdots \times \mathbb{F}_p[x]/f_m(x)$$

if pairwise co-prime and sum of degrees is $2n-1$

$$\mathbb{F}_p[x]/f(x) \times \mathbb{F}_p[x]/f(x) \longrightarrow \mathbb{F}_p[x]/f(x)$$

$$\begin{array}{ccccc} \mathbb{F}_p[x]/f(x) & \times & \mathbb{F}_p[x]/f(x) & \longrightarrow & \mathbb{F}_p[x]/f(x) \\ \rotatebox{90}{$\cong$} & & & & \\ \mathbb{F}_p[x]_{<\deg(f)} & & & & \end{array}$$

$$\begin{tikzcd}
\mathbb{F}_p[x]/f(x) \arrow[d, phantom, "\cong" rotate=90] & \times & \mathbb{F}_p[x]/f(x) \arrow[d, phantom, "\cong" rotate=90] \arrow[r] & \mathbb{F}_p[x]/f(x) \\
\mathbb{F}_p[x]_{<\deg(f)} & \times & \mathbb{F}_p[x]_{<\deg(f)} &
\end{tikzcd}$$

$$
\begin{tikzcd}
\mathbb{F}_p[x]/f(x) \times \mathbb{F}_p[x]/f(x) \arrow[r] & \mathbb{F}_p[x]/f(x) \\
\mathbb{F}_p[x]_{<\deg(f)} \times \mathbb{F}_p[x]_{<\deg(f)} \arrow[u, phantom, "\cong"] \arrow[r] & \mathbb{F}_p[x]_{<2\deg(f)-1} \arrow[u, "\mathrm{mod}"']
\end{tikzcd}
$$

$$R(\mathbb{F}_p[x]/f(x)) \leq P_{\deg(f),\deg(f)}$$

$$\begin{array}{ccccc}
\mathbb{F}_p[x]/f(x) & \times & \mathbb{F}_p[x]/f(x) & \longrightarrow & \mathbb{F}_p[x]/f(x) \\
\cong & & \cong & & \uparrow \text{mod} \\
\mathbb{F}_p[x]_{<\deg(f)} & \times & \mathbb{F}_p[x]_{<\deg(f)} & \longrightarrow & \mathbb{F}_p[x]_{<2\deg(f)-1}
\end{array}$$

$$
\begin{tikzcd}
\mathbb{F}_p[x]/f(x) \times \mathbb{F}_p[x]/f(x) \arrow[r] & \mathbb{F}_p[x]/f(x) \\
\mathbb{F}_p[x]_{<\deg(f)} \times \mathbb{F}_p[x]_{<\deg(f)} \arrow[u, phantom, "\cong"] \arrow[r] & \mathbb{F}_p[x]_{<2\deg(f)-1} \arrow[u, "\mathrm{mod}"']
\end{tikzcd}
$$

$$\begin{tikzcd}
\mathbb{F}_p[x]/f(x) \times \mathbb{F}_p[x]/f(x) \arrow[r] & \mathbb{F}_p[x]/f(x) \\
\mathbb{F}_p[x]_{<\deg(f)} \times \mathbb{F}_p[x]_{<\deg(f)} \arrow[u, phantom, "\cong"] \arrow[r] & \mathbb{F}_p[x]_{<2\deg(f)-1} \arrow[u, "\mathrm{mod}"']
\end{tikzcd}$$

$$R(\mathbb{F}_p[x]/f(x)) \leq P_{\deg(f),\deg(f)}$$

Lempel, Seroussi, and Winograd, 1983

Lempel, Seroussi, and Winograd, 1983

$$P_{n,n} \leq \sum_{i=1}^{m} P_{\deg(f_i),\deg(f_i)}$$

if pairwise co-prime and sum of degrees is $2n-1$

$$F_3 \leq 6$$

$$F_3 \leq 6$$

$$p \geq 2 \cdot 3 - 2 = 4$$

$$F_3 \leq 6$$

$$p \geq 2 \cdot 3 - 2 = 4$$

$$\Downarrow$$

$$P_{3,3} = 2 \cdot 3 - 1 = 5$$

$$F_3 \leq 6$$

$$p \geq 2 \cdot 3 - 2 = 4$$

$$\Downarrow$$

$$F_3 \leq P_{3,3} = 2 \cdot 3 - 1 = 5$$

$$F_3 \leq 6$$

$$p = 2$$

$$F_3 \leq 6$$

$$p = 2$$

$$P_{n,n} \leq \sum_{i=1}^{m} P_{\deg(f_i),\deg(f_i)}$$

$$F_3 \leq 6$$

$$p = 2$$

$$P_{n,n} \leq \sum_{i=1}^{m} P_{\deg(f_i),\deg(f_i)}$$

$$F_3 \leq 6$$

$$p = 2$$

$$P_{n,n} \leq \sum_{i=1}^{m} P_{\deg(f_i),\deg(f_i)}$$

$$f_1 = x$$

$$f_2 = x - 1$$

$$f_3 = x - \infty$$

$$f_4 = x^2 + x + 1$$

$$F_3 \leq 6$$

$$p = 2$$

$$P_{3,3} \leq P_{1,1} + P_{1,1} + P_{1,1} + P_{2,2} = 6$$

$$f_1 = x$$

$$f_2 = x - 1$$

$$f_3 = x - \infty$$

$$f_4 = x^2 + x + 1$$

$$F_3 \leq 6$$

$$p = 3$$

Similar deal

$$F_5$$

$$9 = 1 + 1 + 1 + 3 + 3$$

$$F_5 \leq 1 + 1 + 1 + 6 + 6 = 15$$

$$F_6$$

$$11 = 1 + 1 + 1 + 2 + 3 + 3$$

$$F_6 \leq 1 + 1 + 1 + 3 + 6 + 6 = 18$$

n	naive	K-O	LB
1	1	1	1
2	4	3	3
3	9	7	6
4	16	9	8
5	25	19	10
6	36	21	12
7	49	27	14
8	64	27	16
9	81	55	18
10	100	57	20

n	naive	K-O	CHR	LB
1	1	1	1	1
2	4	3	3	3
3	9	7	6	6
4	16	9	9	8
5	25	19	15	10
6	36	21	18	12
7	49	27	25	14
8	64	27	27	16
9	81	55	33	18
10	100	57	36	20

Montgomery, 2005

n	naive	K-O	CHR	LB
1	1	1	1	1
2	4	3	3	3
3	9	7	6	6
4	16	9	9	8
5	25	19	13	10
6	36	21	17	12
7	49	27	23	14
8	64	27	27	16
9	81	55	33	18
10	100	57	36	20

Lempel, Seroussi, and Winograd, 1983

$$F_n = O(n \log^*(n))$$

1978

Roger Brockett

David Dobkin

$$\forall a \in \mathbb{F}_{p^n}, b \in \mathbb{F}_{p^n}: \qquad ab = \sum_{i=1}^{r} f_i(a) g_i(b) w_i$$

$$\forall a \in \mathbb{F}_{p^n}, b \in \mathbb{F}_{p^n}: \qquad ab = \sum_{i=1}^{r} f_i(a) g_i(b) w_i$$

$$C = \{(f_1(a), f_2(a), \ldots, f_r(a)) \mid a \in \mathbb{F}_{p^n}\}$$

$$\forall a \in \mathbb{F}_{p^n}, b \in \mathbb{F}_{p^n}: \qquad ab = \sum_{i=1}^{r} f_i(a) g_i(b) w_i$$

$$C = \{(f_1(a), f_2(a), \ldots, f_r(a)) \mid a \in \mathbb{F}_{p^n}\}$$

$$\dim\langle f_1, \ldots, f_r \rangle = n$$

$$\forall a \in \mathbb{F}_{p^n}, b \in \mathbb{F}_{p^n}: \qquad ab = \sum_{i=1}^{r} f_i(a) g_i(b) w_i$$

$$C = \{(f_1(a), f_2(a), \ldots, f_r(a)) \mid a \in \mathbb{F}_{p^n}\}$$

$$\dim(C) = n$$

$$\forall a \in \mathbb{F}_{p^n}, b \in \mathbb{F}_{p^n} : \qquad ab = \sum_{i=1}^{r} f_i(a) g_i(b) w_i$$

$$C = \{(f_1(a), f_2(a), \ldots, f_r(a)) \mid a \in \mathbb{F}_{p^n}\}$$

$$\dim(C) = n$$

$$0 \neq a \Rightarrow \dim a\mathbb{F}_{p^n} = n$$

$$\forall a \in \mathbb{F}_{p^n}, b \in \mathbb{F}_{p^n} : \qquad ab = \sum_{i=1}^{r} f_i(a) g_i(b) w_i$$

$$C = \{(f_1(a), f_2(a), \ldots, f_r(a)) \mid a \in \mathbb{F}_{p^n}\}$$

$$\dim(C) = n$$

$$\#\{i \mid f_i(a) \neq 0\} \geq n$$

$$\forall a \in \mathbb{F}_{p^n}, b \in \mathbb{F}_{p^n}: \qquad ab = \sum_{i=1}^{r} f_i(a) g_i(b) w_i$$

$$C = \{(f_1(a), f_2(a), \ldots, f_r(a)) \mid a \in \mathbb{F}_{p^n}\}$$

C is $[r, n, \geq n]_2$-code

$$\forall a \in \mathbb{F}_{p^n}, b \in \mathbb{F}_{p^n}: \qquad ab = \sum_{i=1}^{r} f_i(a) g_i(b) w_i$$

$$C = \{(f_1(a), f_2(a), \ldots, f_r(a)) \mid a \in \mathbb{F}_{p^n}\}$$

$$r \geq \min\{m \mid \exists\, [m, n, \geq n]_2\text{-code}\}$$

$$\min\{m \mid \exists\, [m, n, \geq n]_2\text{-code}\} =: N(n)$$

$$\min\{m \mid \exists\, [m, n, \geq n]_2\text{-code}\} =: N(n)$$

$$N(4) = 8$$

$$N(5) = 12$$

$$N(6) = 14$$

$$N(7) = 17$$

n	naive	K-O	CHR	LB
1	1	1	1	1
2	4	3	3	3
3	9	7	6	6
4	16	9	9	8
5	25	19	13	12
6	36	21	17	14
7	49	27	23	17
8	64	27	27	19
9	81	55	33	24
10	100	57	36	26

Brown and Dobkin, 1980

$$p = 2 \implies F_n \geq 3.527n - o(n)$$

Baur, Bshouty and Kaminski, 1990

$$F_n \geq 3n - o(n)$$

$$F_n = O(n \log^*(n))$$

$$F_n = O(n \log^*(n))$$

$$F_n = \Omega(n)$$

$$F_n = O(n \log^*(n))$$

gap

$$F_n = \Omega(n)$$

End if ideas?

Algorithms of length $2n$-1 correspond to Reed-Solomon codes

Algorithms of length $2n$-1 correspond to Reed-Solomon codes

Algorithms of length $2n$-1 correspond to Reed-Solomon codes

Reed-Solomon codes can be generalized to Algebraic-Geometric codes

Algorithms of length $2n$-1 correspond to
Reed-Solomon codes

Reed-Solomon codes can be generalized to
Algebraic-Geometric codes

Algorithms of length $2n$-1 correspond to Reed-Solomon codes

Reed-Solomon codes can be generalized to Algebraic-Geometric codes

Algorithms?

1988

Gregory and David Chudnovsky

$$\mathbb{F}_{p^n} \times \mathbb{F}_{p^n} \xrightarrow{\Pi_n} \mathbb{F}_{p^n}$$

$$\mathbb{F}_{p^n} \times \mathbb{F}_{p^n} \xrightarrow{\Pi_n} \mathbb{F}_{p^n}$$

$$\mathbb{F}_p[x]_{<n} \times \mathbb{F}_p[x]_{<n} \xrightarrow{\Phi_{n,n}} \mathbb{F}_p[x]_{<2n-1}$$

$$\begin{tikzcd}
\mathbb{F}_{p^n} \times \mathbb{F}_{p^n} \arrow[r, "\Pi_n"] & \mathbb{F}_{p^n} \\
\mathbb{F}_p[x]_{<n} \times \mathbb{F}_p[x]_{<n} \arrow[u] \arrow[r, "\Phi_{n,n}"] & \mathbb{F}_p[x]_{<2n-1} \arrow[u]
\end{tikzcd}$$

$$
\begin{tikzcd}
\mathbb{F}_{p^n} & \times & \mathbb{F}_{p^n} \arrow[r, "\Pi_n"] & \mathbb{F}_{p^n} \\
\mathbb{F}_p[x]_{<n} \arrow[u] & \times & \mathbb{F}_p[x]_{<n} \arrow[u] \arrow[r, "\Phi_{n,n}"] & \mathbb{F}_p[x]_{<2n-1} \arrow[u] \\
\mathbb{F}_p^r & \times & \mathbb{F}_p^r \arrow[r, "\langle r \rangle", "\text{pointwise mult.}"'] & \mathbb{F}_p^r
\end{tikzcd}
$$

$$
\begin{tikzcd}
\mathbb{F}_{p^n} & \times & \mathbb{F}_{p^n} \arrow[r, "\Pi_n"] & \mathbb{F}_{p^n} \\
\mathbb{F}_p[x]_{<n} \arrow[u] \arrow[d] & \times & \mathbb{F}_p[x]_{<n} \arrow[u] \arrow[d] \arrow[r, "\Phi_{n,n}"] & \mathbb{F}_p[x]_{<2n-1} \arrow[u] \arrow[d] \\
\mathbb{F}_p^r & \times & \mathbb{F}_p^r \arrow[r, "\langle r \rangle", "\text{pointwise mult.}"'] & \mathbb{F}_p^r
\end{tikzcd}
$$

$$
\begin{tikzcd}
\mathbb{F}_{p^n} & \times & \mathbb{F}_{p^n} \arrow[r, "\Pi_n"] & \mathbb{F}_{p^n} \\
\mathbb{F}_p[x]_{<n} \arrow[u, two heads] \arrow[d] & \times & \mathbb{F}_p[x]_{<n} \arrow[u, two heads] \arrow[d] \arrow[r, "\Phi_{n,n}"] & \mathbb{F}_p[x]_{<2n-1} \arrow[u] \arrow[d] \\
\mathbb{F}_p^r & \times & \mathbb{F}_p^r \arrow[r, "\langle r \rangle", "\text{pointwise mult.}"'] & \mathbb{F}_p^r
\end{tikzcd}
$$

$$
\begin{tikzcd}
\mathbb{F}_{p^n} \arrow[r, phantom, "\times"] & \mathbb{F}_{p^n} \arrow[r, "\Pi_n"] & \mathbb{F}_{p^n} \\
\mathbb{F}_p[x]_{<n} \arrow[u, two heads] \arrow[d] \arrow[r, phantom, "\times"] & \mathbb{F}_p[x]_{<n} \arrow[u, two heads] \arrow[d] \arrow[r, "\Phi_{n,n}"] & \mathbb{F}_p[x]_{<2n-1} \arrow[u] \arrow[d, hook] \\
\mathbb{F}_p^r \arrow[r, phantom, "\times"] & \mathbb{F}_p^r \arrow[r, "\langle r \rangle", "\text{pointwise mult.}"'] & \mathbb{F}_p^r
\end{tikzcd}
$$

$$R(\Pi_n) \leq R(\Phi_{n,n}) \leq R(\langle r \rangle) = r$$

$$\Uparrow$$

$$\begin{tikzcd}
\mathbb{F}_{p^n} & \times & \mathbb{F}_{p^n} \arrow[r, "\Pi_n"] & \mathbb{F}_{p^n} \\
\mathbb{F}_p[x]_{<n} \arrow[u, two heads] \arrow[d] & \times & \mathbb{F}_p[x]_{<n} \arrow[u, two heads] \arrow[d] \arrow[r, "\Phi_{n,n}"] & \mathbb{F}_p[x]_{<2n-1} \arrow[u] \arrow[d, hook] \\
\mathbb{F}_p^r & \times & \mathbb{F}_p^r \arrow[r, "\langle r \rangle", "\text{pointwise mult.}"'] & \mathbb{F}_p^r
\end{tikzcd}$$

$$
\begin{tikzcd}
\mathbb{F}_{p^n} & \times & \mathbb{F}_{p^n} \arrow[r, "\Pi_n"] & \mathbb{F}_{p^n} \\
\mathbb{F}_p[x]_{<n} \arrow[u, two heads] \arrow[d] & \times & \mathbb{F}_p[x]_{<n} \arrow[u, two heads] \arrow[d] \arrow[r, "\Phi_{n,n}"] & \mathbb{F}_p[x]_{<2n-1} \arrow[u] \arrow[d, hook] \\
\mathbb{F}_p^r & \times & \mathbb{F}_p^r \arrow[r, "\langle r \rangle", "\text{pointwise mult.}"'] & \mathbb{F}_p^r
\end{tikzcd}
$$

$$
\begin{tikzcd}
\mathbb{F}_{p^n} & \times & \mathbb{F}_{p^n} \arrow[r, "\Pi_n"] & \mathbb{F}_{p^n} \\
\mathbb{F}_p[x]_{<n} \arrow[u, twoheadrightarrow] \arrow[d] & \times & \mathbb{F}_p[x]_{<n} \arrow[u, twoheadrightarrow] \arrow[d] \arrow[r, "\Phi_{n,n}"] & \mathbb{F}_p[x]_{<2n-1} \arrow[u] \arrow[d, hook] \\
\mathbb{F}_p^r & \times & \mathbb{F}_p^r \arrow[r, "\langle r \rangle", "\text{pointwise mult.}"'] & \mathbb{F}_p^r
\end{tikzcd}
$$

$$
\begin{tikzcd}
\mathbb{F}_{p^n} & \times & \mathbb{F}_{p^n} \arrow[r, "\Pi_n"] & \mathbb{F}_{p^n} \\
\mathbb{F}_p[x]_{<n} \arrow[u, two heads] \arrow[d] & \times & \mathbb{F}_p[x]_{<n} \arrow[u, two heads] \arrow[d] \arrow[r, "\Phi_{n,n}"] & \mathbb{F}_p[x]_{<2n-1} \arrow[u] \arrow[d, hook] \\
\mathbb{F}_p^r & \times & \mathbb{F}_p^r \arrow[r, "\langle r \rangle", "\text{pointwise mult.}"'] & \mathbb{F}_p^r
\end{tikzcd}
$$

$\mathbb{F}_p[x]_{<n}$ Functions with only pole at infinity of order < *n*

Projective line

Smooth projective algebraic curve

Smooth projective algebraic curve

Smooth projective algebraic curve

$$\alpha_1, \ldots, \alpha_n$$

Smooth projective algebraic curve

Points $P_1, \ldots, P_n$ on the curve

Smooth projective algebraic curve

Points $P_1, \ldots, P_n$ on the curve

Smooth projective algebraic curve

Points $P_1, \ldots, P_n$ on the curve

$$\mathbb{F}_p[x]_{<n}$$

Smooth projective algebraic curve

Points $P_1, \ldots, P_n$ on the curve

$$\mathcal{L}(D)$$

Smooth projective algebraic curve

Points $P_1, \ldots, P_n$ on the curve

$\mathcal{L}(D)$

$$
\begin{tikzcd}
\mathbb{F}_{p^n} & \times & \mathbb{F}_{p^n} \arrow[r, "\Pi_n"] & \mathbb{F}_{p^n} \\
\mathcal{L}(D) \arrow[u, two heads] \arrow[d] & \times & \mathcal{L}(D) \arrow[u, two heads] \arrow[d] \arrow[r] & \mathcal{L}(2D) \arrow[u] \arrow[d, hook] \\
\mathbb{F}_p^r & \times & \mathbb{F}_p^r \arrow[r, "\langle r \rangle"] & \mathbb{F}_p^r
\end{tikzcd}
$$

$$
\begin{tikzcd}
\mathbb{F}_{p^n} & \times & \mathbb{F}_{p^n} \arrow[r, "\Pi_n"] & \mathbb{F}_{p^n} \\
\mathcal{L}(D) \arrow[u, two heads] \arrow[d] & \times & \mathcal{L}(D) \arrow[u, two heads] \arrow[d] \arrow[r] & \mathcal{L}(2D) \arrow[u] \arrow[d, hook] \\
\mathbb{F}_p^r & \times & \mathbb{F}_p^r \arrow[r, "\langle r \rangle"] & \mathbb{F}_p^r
\end{tikzcd}
$$

$$\deg(D) \geq n + 2g \;\Rightarrow\; \mathcal{L}(D) \twoheadrightarrow \mathbb{F}_{p^n}$$

$$\begin{tikzcd}
\mathbb{F}_{p^n} & \times & \mathbb{F}_{p^n} \arrow[r, "\Pi_n"] & \mathbb{F}_{p^n} \\
\mathcal{L}(D) \arrow[u, two heads] \arrow[d] & \times & \mathcal{L}(D) \arrow[u, two heads] \arrow[d] \arrow[r] & \mathcal{L}(2D) \arrow[u] \arrow[d, hook] \\
\mathbb{F}_p^r & \times & \mathbb{F}_p^r \arrow[r, "\langle r \rangle"] & \mathbb{F}_p^r
\end{tikzcd}$$

$$\deg(D) \geq n + 2g \;\Rightarrow \mathcal{L}(D) \twoheadrightarrow \mathbb{F}_{p^n}$$

Curve has at least *r* points and $\deg(D) < \dfrac{r}{2}$

$$
\begin{tikzcd}
\mathbb{F}_{p^n} \times \mathbb{F}_{p^n} \arrow[r, "\Pi_n"] & \mathbb{F}_{p^n} \\
\mathcal{L}(D) \times \mathcal{L}(D) \arrow[u, two heads] \arrow[d] \arrow[r] & \mathcal{L}(2D) \arrow[u] \arrow[d, hook] \\
\mathbb{F}_p^r \times \mathbb{F}_p^r \arrow[r, "\langle r \rangle"] & \mathbb{F}_p^r
\end{tikzcd}
$$

$$n < \frac{r}{2} - 2g \Rightarrow \Pi_n \leq r$$

$$\begin{tikzcd}
\mathbb{F}_{p^n} & \times & \mathbb{F}_{p^n} \arrow[r, "\Pi_n"] & \mathbb{F}_{p^n} \\
\mathcal{L}(D) \arrow[u, two heads] \arrow[d] & \times & \mathcal{L}(D) \arrow[u, two heads] \arrow[d] \arrow[r] & \mathcal{L}(2D) \arrow[u] \arrow[d, hook] \\
\mathbb{F}_p^r & \times & \mathbb{F}_p^r \arrow[r, "\langle r \rangle"] & \mathbb{F}_p^r
\end{tikzcd}$$

$$n < \frac{r}{2} - 2g \Rightarrow \Pi_n \leq r$$

$$\frac{g}{r} \text{ bounded} \Longrightarrow F_n = O(n)$$

Modular curves

$$F_n = O(n)$$

Extensions by

Extensions by

S. - 1991-1993

Shparlinski, Tsfasman, Vladut - 1992

Ballet et al. - 1999 - 2005

Some Open Questions

Some Open Questions

Exact asymptotic order of F_n

Some Open Questions

Exact asymptotic order of F_n

Better lower bounds

Some Open Questions

Exact asymptotic order of F_n

Better lower bounds

Use of triples of codes rather than one

Some Open Questions

Exact asymptotic order of F_n

Better lower bounds

Use of triples of codes rather than one

Are F_n and $P_{n,n}$ equal?

Some Open Questions

Exact asymptotic order of F_n

Better lower bounds

Use of triples of codes rather than one

Are F_n and $P_{n,n}$ equal?

Applications to the MDS conjecture?