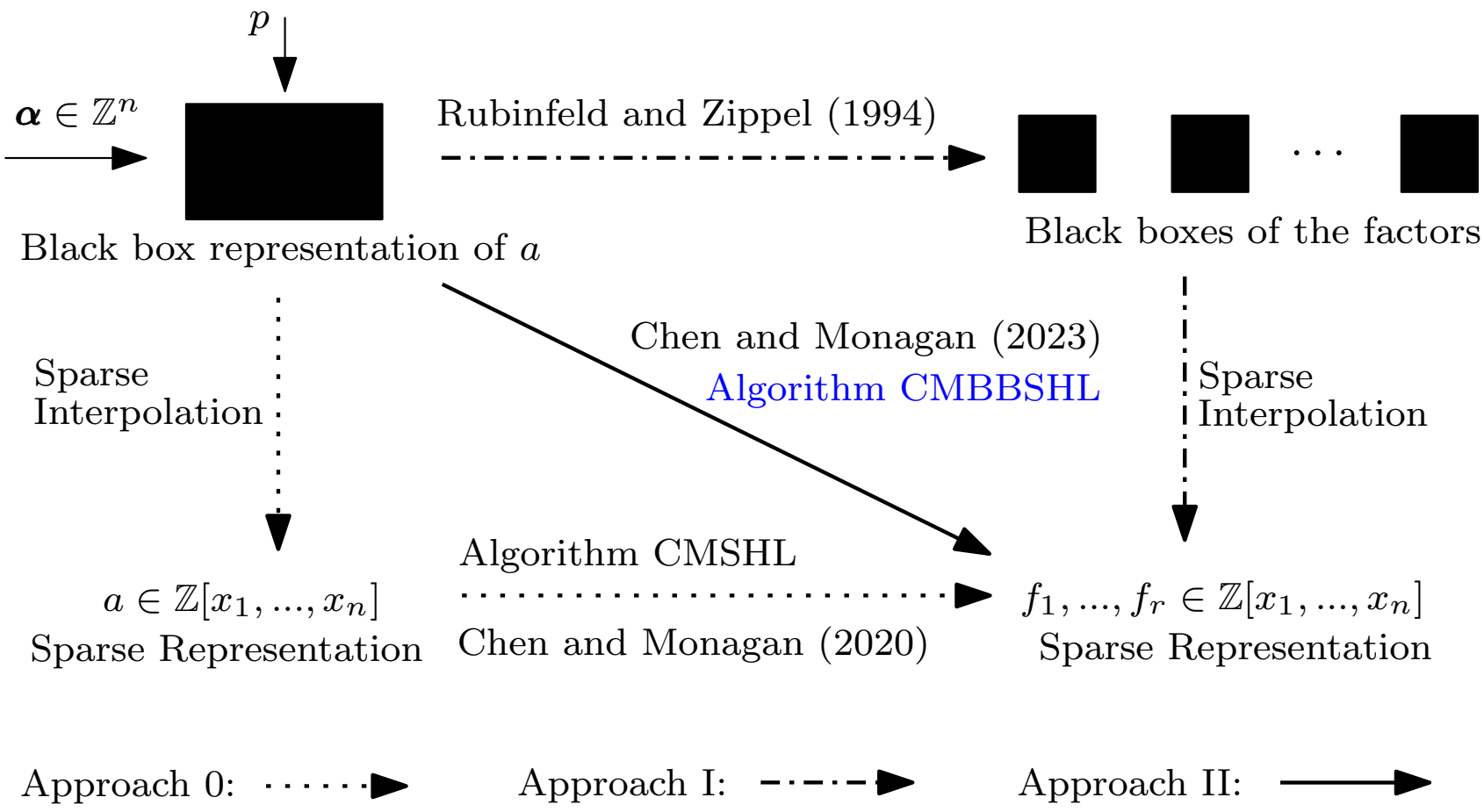
Computing the factors of the content using a black box representation

Tian Chen and Michael Monagan

Department of Mathematics,
Simon Fraser University, Canada

Black box factorization



Factoring the content recursively

Let $\mathcal{C}_n = a \in \mathbb{Z}[x_1, \cdots, x_n]$. We have $\mathcal{C}_n = \mathrm{cont}(\mathcal{C}_n) \cdot \mathrm{pp}(\mathcal{C}_n)$.

$\mathrm{pp}(\mathcal{C}_n) = \prod_{\rho=1}^{r} f_\rho^{e_\rho}$. f_ρ's are irreducible over $\mathbb{Z}$ and primitive in x_1.

Let $\mathcal{C}_{n-1} = \mathrm{cont}(\mathcal{C}_n) \in \mathbb{Z}[x_2, \cdots, x_n]$.

- After factoring $\mathrm{pp}(\mathcal{C}_n)$, we create a black box $\mathsf{F}_n : \mathbb{Z}^n \times \{p\} \to \mathbb{Z}_p$ s.t. $\mathsf{F}_n(\boldsymbol{\alpha}, p) = \mathrm{pp}(\mathcal{C}_n)(\boldsymbol{\alpha}) \bmod p$ by computing

$$\mathrm{pp}(\mathcal{C}_n)(\boldsymbol{\alpha}) \bmod p = f_1(\boldsymbol{\alpha})^{e_1} \cdots f_r(\boldsymbol{\alpha})^{e_r} \bmod p.$$

- Next, we create another black box $\mathsf{C}_{n-1} : \mathbb{Z}^{n-1} \times \{p\} \to \mathbb{Z}_p$ for the content $\mathcal{C}_{n-1} = \mathrm{cont}(\mathcal{C}_n)$ s.t.

$$\mathsf{C}_{n-1}(\boldsymbol{\beta}, p) = \frac{\mathsf{C}_n([\gamma, \boldsymbol{\beta}], p)}{\mathsf{F}_n([\gamma, \boldsymbol{\beta}], p)} \bmod p$$

  for a fixed $\gamma \in \mathbb{Z}$. If $\mathsf{F}_n([\gamma, \boldsymbol{\beta}], p) = 0$ then FAIL is returned.
- Then the content is factored recursively. $\mathcal{C}_0 \in \mathbb{Z}$.

```
MakeCont := proc( C::procedure, F::procedure, gamma::integer,
p::prime )
    proc( alpha::Array, p::prime )
        local na := numelems(alpha), alphaNew, g;
        alphaNew := Array(1..na+1);
        alphaNew[1] := gamma;
        for i to na do alphaNew[i+1] := alpha[i]; od;
        g := F( alphaNew, p );
        if g = 0 then return FAIL; fi;
        C( alphaNew, p )/g mod p;
    end;
end;
gamma0 := rand(p)();
BBC := MakeCont( Cn, Fn, gamma0, p );
```

Example

Let V_n be an $n \times n$ Vandermonde matrix. E.g.

$$V_4 = \begin{pmatrix} 1 & x_1 & x_1^2 & x_1^3 \\ 1 & x_2 & x_2^2 & x_2^3 \\ 1 & x_3 & x_3^2 & x_3^3 \\ 1 & x_4 & x_4^2 & x_4^3 \end{pmatrix}.$$

$\det(V_4)$ has 6 linear factors. In general, $\det(V_n)$ has $\binom{n}{2}$ linear factors. $\#\text{expand}(\det(V_4)) = 24$.

$$\mathcal{C}_4 = \det(V_4) = \underbrace{(x_3 - x_4)(x_2 - x_3)(x_2 - x_4)}_{\mathcal{C}_3 = \text{cont}(\mathcal{C}_4)} \underbrace{(x_1 - x_2)(x_1 - x_3)(x_1 - x_4)}_{\text{pp}(\mathcal{C}_4)},$$

$$\mathcal{C}_3 = \underbrace{(x_3 - x_4)}_{\mathcal{C}_2 = \text{cont}(\mathcal{C}_3)} \underbrace{(x_2 - x_3)(x_2 - x_4)}_{\text{pp}(\mathcal{C}_3)},$$

$$\mathcal{C}_2 = \underbrace{x_3 - x_4}_{\text{pp}(\mathcal{C}_2)},$$

$$\mathcal{C}_1 = \text{cont}(\mathcal{C}_2) = 1,$$

$$\mathcal{C}_0 = \text{cont}(\mathcal{C}_1) = 1.$$

Timings

$n = N$	7	8	9	10	11	12	13
$r = \binom{n}{2}$	21	28	36	45	55	66	78
$\#\det(V_n)$	5040	40320	362880	3628800	39916800	O/M*	N/A
CMBBSHL	0.336	0.649	1.137	1.990	3.290	5.190	8.175
probes tot	1328	2256	3597	5467	7975	11263	15479
Maple det	0.061	0.100	0.446	5.700	45.07	O/M	N/A
det minor	0.009	0.036	0.297	5.391	35.518	O/M	N/A
Maple fac	0.012	0.068	0.882	17.96	523.80	N/A	N/A
Maple tot	0.021	0.104	1.179	23.351	559.318	N/A	N/A

Table: CPU timings (in seconds) for computing the factors of $\det(V_n)$. N/A: Not attempted. O/M: $>$ 64 gigs. O/M*: Out of memory at expanding the factors in Maple.

$n = N$	7	8	9	10	11	12	13
CMBBSHL tot	0.366	0.649	1.137	1.990	3.290	5.190	8.175
probes tot	1328	2256	3597	5467	7975	11263	15479
$\mathrm{pp}(a)$ fac	0.097	0.130	0.175	0.262	0.331	0.401	0.513
$\mathrm{pp}(C_i)$ fac	0.098	0.180	0.263	0.369	0.593	0.808	1.140
$(i = n-1, \cdots, 0)$	0.097	0.137	0.246	0.426	0.654	0.924	1.348
	0.045	0.100	0.213	0.411	0.541	0.913	1.348
	0.021	0.065	0.127	0.237	0.474	0.746	1.155
	0.005	0.026	0.070	0.153	0.351	0.577	0.984
	0.000	0.005	0.030	0.083	0.190	0.370	0.707
	0.002	0.000	0.007	0.036	0.100	0.267	0.495
	-	0.001	0.000	0.008	0.042	0.115	0.267
	-	-	0.002	0.000	0.009	0.051	0.142
	-	-	-	0.002	0.001	0.011	0.056
	-	-	-	-	0.002	0.000	0.012
	-	-	-	-	-	0.003	0.000
	-	-	-	-	-	-	0.003

Table: CPU timings (in seconds) for computing the factors of $\mathrm{pp}(C_i)$.

$n = N$	15	20	25	30	35	40
$r = \binom{n}{2}$	105	190	300	435	595	780
CMBBSHL tot	18.625	109.996	440.17	1376.793	3560.706	9057.977
probes tot	27311	85622	207912	429752	793809	1350786
$\mathrm{pp}(a)$ fac	0.791	2.246	5.891	13.968	29.597	57.745
H.L. x_n	0.055	0.117	0.256	0.467	0.800	1.487
probes x_n	465	820	1275	1830	2485	3240
s (H.L. x_n)	1	1	1	1	1	1
BB tot	0.024	0.070	0.156	0.353	0.650	1.224
BB eval	0.015	0.039	0.090	0.208	0.368	0.709
BB det	0.009	0.031	0.066	0.145	0.282	0.515
Interp2var	0.001	0.002	0.004	0.009	0.015	0.027
Eval $\hat{f}_{\rho_j - 1}$	0.002	0.002	0.003	0.004	0.004	0.005
BHL	0.004	0.005	0.008	0.009	0.010	0.011
VSolve	0.004	0.003	0.006	0.009	0.007	0.012

Table: CPU timings (sec) for computing the factors of $\det(V_n)$ for larger n.

References

Chen, T., Monagan, M.:
The complexity and parallel implementation of two sparse multivariate Hensel lifting algorithms for polynomial factorization.
In Proceedings of CASC '20, LNCS **12291**, 150–169. Springer (2020)

Chen, T., Monagan, M.:
A new black box factorization algorithm – the non-monic case.
To appear in Proceedings of ISSAC '23.

Rubinfeld, R., Zippel, R.E.:
A new modular interpolation algorithm for factoring multivariate polynomials.
In Proceedings of Algorithmic Number Theory, First International Symposium, ANTS-I (1994)