Computational Aspects of Zero-Dimensional Schemes

K field

$\mathbb{P}^n$ projective n-space over K

$\mathbb{X} = \{P_1, \ldots, P_s\}$ set of s K-rational points

$P_i = (p_{i0} : \ldots : p_{in})$ with $p_{ij} \in K$

$A = K[x_0, \ldots, x_n]$ polynomial ring over K

$I_{\mathbb{X}} \subseteq A$ homogeneous vanishing ideal of X

$R = A/I_{\mathbb{X}}$ homogeneous coordinate ring of $\mathbb{X}$

$\mathrm{HF}_{\mathbb{X}} : \mathbb{Z} \longrightarrow \mathbb{N}$ $(i \mapsto \dim_K(R_i))$ Hilbert function of $\mathbb{X}$

$\mathbb{T}^{n+1}$ set of terms (power products, monomials) in A

σ term ordering on $\mathbb{T}^{n+1}$

1 Computing the Homogeneous Vanishing Ideal

Problem. Given the coordinates p_{ij} of the points, compute the homogeneous vanishing ideal $I_{\mathbb{X}} = I_{P_1} \cap \cdots I_{P_s}$

Classical Solution. Since we know

$$I_{P_i} = (p_{ij}x_k - p_{ik}x_j \mid 0 \le j < k \le n)$$

we can use Gröbner bases to compute the intersection $I_{P_1} \cap \cdots \cap I_{P_s}$.

But for $s >> 0$, this is computationally expensive, because the Gröbner bases become huge.

Idea. The classical Buchberger-Möller algorithm gives us a way to compute the vanishing ideal of an affine set of points using linear algebra. It is very efficient.

We want to mimick the procedure and compute the intersection of the 1-dimensional ideals $I_{P_1}, \ldots, I_{P_s}$ degree by degree. In each degree we are dealing with a finite-dimensional vector space and linear algebra methods apply.

Definition 1.1. For a computation which proceeds degree by degree, a **stopping criterion** is a logical condition which depends only on the data obtained in the computation up to the current degree d, and which, if satisfied, guarantees that the result computed so far is complete.

Proposition 1.2 (Primitive Stopping Criterion)
If we have computed a σ-Gröbner basis of $I_{\mathbb{X}}$ up to degree s, the result is complete.

Theorem 1.3 (The Projective BM-Algorithm)
Assume that there exists a function `StoppingCriterion`(G) *which returns* `TRUE` *if the set* G *computed so far is a* σ*-Gröbner basis of* $I_{\mathbb{X}} = I_{P_1} \cap \cdots \cap I_{P_s}$*, and* `FALSE` *otherwise.*

Consider the following sequence of instructions.

PBM1 *Start with empty lists* $G = [\,]$*,* $H = [\,]$*, a list* $L = [1]$*, and* $d = 0$*.*

PBM2 *Apply the function* `StoppingCriterion`(G)*. If it returns* `TRUE`*, return the list* G *and stop. Otherwise increase* d *by one, set* $M = (m_{ij})$ *to be a matrix over* K *with zero rows and* s *columns, and let* L *be the list of all terms of degree* d *which are not multiples of any element of* $\{\mathrm{LT}_\sigma(g) \mid g \in G\}$*.*

PBM3 *If* $L = \emptyset$*, go to step PBM2. Otherwise choose the term* $t = \min_\sigma(L)$ *and remove it from* L*.*

PBM4 *Compute the vector* $\mathbf{v} = (t(P_1), \ldots, t(P_s)) \in K^s$ *and reduce it against the rows of* M *to obtain*

$$\mathbf{v}^* = \mathbf{v} - \sum_i a_i\,(m_{i1}, \ldots, m_{is}) \qquad \text{with } \; a_i \in K$$

PBM5 *If* $\mathbf{v}^* = (0, \ldots, 0)$*, then append the polynomial* $t - \sum_i a_i h_i$ *to the list* G*, where* h_i *is the* i^{th} *element of the list* H*. Continue with step PBM3.*

PBM6 *Otherwise* $\mathbf{v}^* \neq 0$*, so append* $\mathbf{v}^*$ *as a new row to* M *and* $t - \sum_i a_i h_i$ *as a new element to* H*. Continue with step PBM3.*

This is an algorithm which returns the reduced σ*-Gröbner basis* G *of the ideal* $I_{\mathbb{X}} = I_{P_1} \cap \cdots \cap I_{P_s}$*.*

Problem. We need a better stopping criterion!

DEFINITION 1.4. Let $\mathbb{T}_d^{n+1}$ be the set of power products of degree d in $K[x_0, \dots, x_n]$, and let $Q \subseteq \mathbb{T}_d^{n+1}$. We say that two power products t, t' are **connected in** Q if there is a sequence of power products $t_0, t_1, \dots, t_r \in Q$ with $t_0 = t$ and $t_r = t'$ such that for each $i = 1, \dots, r$ there exist $\alpha, \beta \in \{0, \dots, n\}$ satisfying $t_i = t_{i-1} \cdot x_\alpha / x_\beta$. The intuitive meaning of this notion is that one can pass from one t_i to the next by replacing one indeterminate by another.

We define the **connected components in** Q in the obvious way; they are clearly disjoint. The connected component of a power product $t \notin Q$ is empty.

Theorem 1.5 (Projective Stopping Criterion)
In the setting of the projective BM-algorithm, suppose we have computed homogeneous polynomials whose leading terms generate $(\mathrm{LT}_\sigma(I_{\mathbb{X}})_{\leq d})$ *for some degree* $d \geq 1$ *and that the following conditions hold:*

a) $\mathrm{HF}_{A/\mathrm{LT}_\sigma(I_{\mathbb{X}})}(d) = s$ *or*
$d > 0$ *and* $\mathrm{HF}_{A/\mathrm{LT}_\sigma(I_{\mathbb{X}})}(d) = \mathrm{HF}_{A/\mathrm{LT}_\sigma(I_{\mathbb{X}})}(d-1)$

b) For $i = 0, \dots, n$, *every power product in the connected component of* x_i^d *in* $(\mathbb{T}^{n+1} \setminus \mathrm{LT}_\sigma(I_{\mathbb{X}}))_d$ *is divisible by* x_i.

Then the homogeneous polynomials computed so far are a σ*-Gröbner basis of* $I_{\mathbb{X}}$.

Problem. The projective BM-algorithm works fine over finite fields, but for $K = \mathbb{Q}$ the coefficients in the matrix M become too large and even linear algebra is slow.

Theorem 1.6 (The Modular BM-Algorithm)
Let $n \geq 1$, let σ be a term ordering on $\mathbb{T}^n$ and $P_i = (p_{i1}, \dots, p_{in}) \in \mathbb{Q}^n$ for $i = 1, \dots, s$. Consider the following instructions.

MBM1 *Let $Q = [\,]$, $G = [\,]$ and $G_m = [\,]$ be empty lists, and let $m = 1$.*

MBM2 *Pick a new prime number p, different from the previous ones and such that the points P_i have distinct reductions $\overline{P}_i$ modulo p*

MBM3 *Apply the classical Buchberger-Möller Algorithm to $K = \mathbb{F}_p$ and the set of points $\{\overline{P}_1, \dots, \overline{P}_s\}$. Denote the result by $[G_p, Q_p]$.*

MBM4 *Compare Q_p with Q in the following way:*
for $Q = [q_1, q_2, \dots]$ and $Q_p = [q'_1, q'_2, \dots]$, we say that Q is **better** *than Q' if for some index j we have $q_i = q'_i$ for $i = 1, 2, \dots, j-1$ and $q_j <_\sigma q'_j$.*
If Q is better *than Q_p then continue with step* MBM2. *If Q_p is* better *than Q then replace Q by Q_p, set m equal to p, put G_p in G_m, then continue with step* MBM2.

MBM5 *At this point we have $Q_p = Q$. Replace m by mp. Update G_m by combining it with G_p using the Chinese Remainder Theorem. Perform rational recovery on G_m with modulus m, and call the result G'.*

MBM6 *If $G' \neq G$ then replace G by G' and continue with* MBM2.

MBM7 *Now $G' = G$. Check whether all polynomials in G vanish at all points of the set $\{P_1, \dots, P_s\}$. If they do not, go back to step* MBM2. *Otherwise return $[G, Q]$ and stop.*

This is an algorithm which returns the reduced σ-Gröbner basis G of $I_{\mathbb{X}}$ and a list of terms Q whose residue classes form a K-basis of $K[x_1, \dots, x_n]/I_{\mathbb{X}}$.

Application: Design of Experiments

Problem. For some experiment, several parameters $\lambda_1, \dots, \lambda_n$ can take finitely many values $\lambda_i \in \{\alpha_{i1}, \dots, \alpha_{i\nu_i}\} \subseteq \mathbb{Q}$ each. The set of all tuples $(\alpha_{1\,j_1}, \dots, \alpha_{n\,j_n}) \in \mathbb{Q}^n$ such that $1 \le j_1 \le \nu_1, \dots, 1 \le j_n \le \nu_n$ is called the **full design** $\mathbb{D}$.

There is an (unknown) function $f : \mathbb{D} \longrightarrow \mathbb{Q}$, called the **model**. We would like to choose a *small* subset $\mathbb{F} \subseteq \mathbb{D}$, called a **fraction** in such a way that we can reconstruct the function f from its restriction $f|_{\mathbb{D}} : \mathbb{F} \longrightarrow \mathbb{Q}$ and some additional information about f. (One says that we want to **identify the model**.)

Mathematical solution method.

a) Since the model $f : \mathbb{D} \longrightarrow \mathbb{Q}$ is defined on a finite set $\mathbb{D}$, it is a polynomial function. The corresponding polynomial $F \in \mathbb{Q}[x_1, \dots, x_n]$ is unique up to addition of elements of $I_{\mathbb{D}}$.

b) The set $\mathbb{D}$ is a very special set of points (a complete intersection), and we know its vanishing ideal

$$I_{\mathbb{D}} = ((x_1 - \alpha_{1\,1}) \cdots (x_1 - \alpha_{1\,\nu_1}, \dots, (x_n - \alpha_{n\,1}) \cdots (x_n - \alpha_{n\,\nu_n}))$$

c) The additional information about the model we have usually concerns the support of F and tells us what the size of $\mathbb{F}$ should be.

d) Try many subsets $\mathbb{F} \subseteq \mathbb{D}$ of the appropriate size. Everytime compute $I_{\mathbb{F}}$ using the modular BM-algorithm and check (using simple linear algebra) whether $\mathbb{F}$ allows us to identify the model.

Literature. 1) J. Abbott, A. Bigatti, M. Kreuzer, and L. Robbiano, Computing ideals of points, J. Symb. Comp. **30** (2000), 341–356

2) L. Robbiano, Gröbner bases and statistics, in: B. Buchberger and F. Winkler (eds.), Gröbner Bases and Applications, LMS Lecture Notes **251**, Cambridege University Press 1998, pp. 179–204

3) J. Abbott, M. Kreuzer, and L. Robbiano, Computing zero-dimensional schemes, J. Symb. Comp. (to appear)

Application: Implicitization

Problem. Suppose we are given $f_1, \ldots, f_s \in K[x_1, \ldots, x_n]$. We want to compute the ideal of all polynomials $g \in K[y_1, \ldots, y_s]$ such that $g(f_1, \ldots, f_s) = 0$.

Classical Solution. Form the ideal

$$J = (y_1 - f_1, \ldots, y_s - f_s) \subseteq K[x_1, \ldots, x_n, y_1, \ldots, y_s]$$

and compute a Gröbner basis of J with respect to some elimination ordering for $\{x_1, \ldots, x_n\}$.

Except for small examples, this method leads to very hard Gröbner basis computations!

New Method. In the spirit of the BM-algorithm, one can proceed as follows.

1) Reduce the computation to the case where all polynomials $f_1, \ldots, f_s$ are homogeneous of the same degree d.
2) Let $\deg(x_i) = 1$ and $\deg(y_j) = d$. Then J is a homogeneous ideal with respect to this grading. For a suitable term ordering, $(y_1, \ldots, y_s)$ is the leading term ideal of J. Hence we know the Hilbert function of J.
3) Compute the kernel of the K-algebra homomorphism

$$\varphi : K[y_1, \ldots, y_s] \longrightarrow K[x_1, \ldots, x_n]$$

   which is defined by $\varphi(y_i) = f_i$ for $i = 1, \ldots, s$. To this end, proceed degree by degree and apply the method of the projective BM-algorithm. Since we know the Hilbert function, we have a stopping criterion.

2 Checking Uniformity Conditions

$\mathbb{X} = \{P_1, \ldots, P_s\}$ set of K-rational points in $\mathbb{P}^n$

$R = A/I_{\mathbb{X}}$ homogeneous coordinate ring of $\mathbb{X}$

$\mathrm{HF}_{\mathbb{X}} : \mathbb{Z} \longrightarrow \mathbb{N}$ Hilbert function of $\mathbb{X}$

$$0 = \mathrm{HF}_{\mathbb{X}}(-1) < 1 = \mathrm{HF}_{\mathbb{X}}(0) < \cdots < \mathrm{HF}_{\mathbb{X}}(a_{\mathbb{X}}) <$$
$$s = \mathrm{HF}_{\mathbb{X}}(a_{\mathbb{X}}+1) = \mathrm{HF}_{\mathbb{X}}(a_{\mathbb{X}}+2) = \cdots$$

DEFINITION 2.1. Let $1 \le i \le s$ and $1 \le j \le a_{\mathbb{X}}$. The scheme $\mathbb{X}$ is called **(i,j)-uniform** if every subscheme $\mathbb{Y} \subseteq \mathbb{X}$ consisting of $s-i$ points satisfies $\mathrm{HF}_{\mathbb{Y}}(j) = \mathrm{HF}_{\mathbb{X}}(j)$.

EXAMPLE 2.2. a) The scheme $\mathbb{X}$ has the Cayley-Bacharach property iff $\mathbb{X}$ is $(1, a_{\mathbb{X}})$-uniform.

b) Suppose that $\mathbb{X}$ spans $\mathbb{P}^n$. Then $\mathbb{X}$ is in linearly general position iff $\mathbb{X}$ is $(s-n-1, 1)$-uniform.

c) $\mathbb{X}$ is in uniform position iff $\mathbb{X}$ is (i,j)-uniform for all i, j.

d) The Gale transform of $\mathbb{X}$ is well-defined iff $\mathbb{X}$ is $(2,1)$-uniform. More generally, the i^{th} canonical transform of $\mathbb{X}$ is well-defined iff $\mathbb{X}$ is $(2,i)$-uniform.

e) The Eisenbud-Green-Harris conjecture asks whether any zero-dimensional complete intersection of quadrics is $(2^{n-j}-1, j)$-uniform for $1 \le j \le a_{\mathbb{X}}$.

REMARK 2.3. a) If $\mathbb{X}$ is (i,j)-uniform, then $\mathbb{X}$ is (k,ℓ)-uniform for all $1 \le k \le i$ and all $1 \le j \le \ell$.

b) If $\mathbb{X}$ is (i,j)-uniform, then we have $i \le s - \mathrm{HF}_{\mathbb{X}}(j)$.

Problem. How can one compute the region of uniformity efficiently?
Answer. In general, this is impossible. The problem is known to be NP-complete. Thus we can only try to find efficient algorithms for special cases.

Proposition 2.4 (Geramita – K – Robbiano)
Let $1 \le i \le \Delta = s - \mathrm{HF}_{\mathbb{X}}(a_{\mathbb{X}})$. Moreover, let $f_1, \dots, f_s \in A_{a_{\mathbb{X}}+1}$ be polynomials whose residue classes in R are the **separators** *of $\mathbb{X}$, i.e. such that $f_j(P_k) = \delta_{jk}$ for $j,k = 1, \dots, s$. Then the following conditions are equivalent:*

a) $\mathbb{X}$ is $(i, a_{\mathbb{X}})$-uniform.

b) The images of any Δ elements of $\{f_1, \dots, f_s\}$ in $R_{a_{\mathbb{X}}+1}$ are K-linearly independent.

c) If one chooses a K-basis $b_1, \dots, b_\Delta$ of $R_{a_{\mathbb{X}}+1}$ and forms the matrix $\mathcal{B}$ whose columns are the coordinate tuples of $\overline{f}_1, \dots, \overline{f}_s$ in that basis, then the maximal minors of $\mathcal{B}$ are all different from zero.

The last condition can be checked efficiently using a recent algorithm of Krammer and K. which uses certain versions of Bareiss' algorithm to compute many maximal minors simultaneously.

Proposition 2.5 *Let $1 \le j \le a_{\mathbb{X}}$. The following conditions are equivalent.*

a) $\mathbb{X}$ is $(s - \mathrm{HF}_{\mathbb{X}}(j), j)$-uniform.

b) The multiplicaiton map $\mu_j : R_j \otimes (\omega_R)_{-j} \longrightarrow (\omega_R)_0$ is 1-generic, i.e. we have $\mu_j(r \otimes w) = 0 \Rightarrow r = 0$ or $w = 0$.

Here ω_R is the **canonical module** of R and can be computed efficiently using the algorithm of Beck – K. Moreover, the second condition can be checked efficiently.

Proposition 2.6 (Geramita – K – Robbiano)
Let $1 \le j \le a_{\mathbb{X}}$*, and suppose that* $\mathbb{X}$ *is* $(s - \mathrm{HF}_{\mathbb{X}}(j), j)$*-uniform. Choose a zero-dimensional complete intersection* $\mathbb{V} = \mathcal{Z}(g_1, \dots, g_n)$ *containing* $\mathbb{X}$ *(for instance a full design!). The set of points* $\mathbb{Y} = \mathbb{V} \setminus \mathbb{X}$ *defined by* $I_{\mathbb{Y}} = I_{\mathbb{V}} :_A I_{\mathbb{X}}$ *is called the* **residual scheme** *of* $\mathbb{X}$ *in* $\mathbb{V}$*. Let* $\alpha = \min\{j \mid (I_{\mathbb{V}})_j \subset (I_{\mathbb{Y}})_j\}$ *be its initial degree in* $\mathbb{V}$*. Then the following conditions are equivalent.*

a) $\mathbb{X}$ *is* $(s - \mathrm{HF}_{\mathbb{X}}(j) + 1, j - 1)$*-uniform.*

b) We have $\left[I_{\mathbb{V}} : (I_{\mathbb{Y}})_{\alpha + a_{\mathbb{X}} - j + 1}\right]_{j-1} = (I_{\mathbb{X}})_{j-1}$*.*

The last condition can be checked efficiently using two truncated Gröbner basis computations. This result has been implemented by T. Eisenmann.

Literature. 1) A.V. Geramita, M. Kreuzer and L. Robbiano, Cayley-Bacharach schemes and their canonical modules, TAMS **339** (1993), 163–189

2) B. Krammer, Algorithmic linear algebra for polynomial matrices (in German), diplom thesis, Regensburg University 2001

3) M. Kreuzer, On the canonical module of a 0-dimensional scheme, Can. J. Math. **46** (1994), 357–379

4) M. Kreuzer, On the canonical ideal of a set of points, Boll. UMI 1-B **8** (2000), 221–261

5) S. Beck and M. Kreuzer, How to compute the canonical module of a set of points, in: L. Gonzales-Vega and T. Recio (eds.), Algorithms in Algebraic Geometry and Applications, Progress in Math. **143**, Birkhäuser Verlag 1996, pp. 51–78

6) T. Eisenmann, Implementation and optimization of algorithms for zero-dimensional schemes (in German), diplom thesis, Regensburg University 2002

Application: Coding Theory

p prime number, $e > 0$, $q = p^e$

$K = \mathbb{F}_q$ finite field having q elements

$C \subseteq K^s$ subvector space is called a **linear code** of length s

$d = \dim_K(C)$ is called the **dimension** of C

$m(C) = \min\{\#\{i \mid c_i \neq 0\} \mid (c_1, \ldots, c_s) \in C \setminus \{0\}\}$ is called the **minimal distance** of C

Proposition 2.7 (Singleton Bound)
For every linear code C we have $m(C) \leq s - d + 1$.

Proposition 2.8 (Hansen's Construction)
Let $\mathbb{X} = \{P_1, \ldots, P_s\} \subseteq \mathbb{P}^n$ be a set of K-rational points and let $1 \leq j \leq a_{\mathbb{X}}$.

a) The image of the K-linear map $\Phi_j : R_j \longrightarrow K^s$ defined by $f \mapsto (f(P_1), \ldots, f(P_s))$ is a linear code of length s and dimension $d = \mathrm{HF}_{\mathbb{X}}(j)$. It is called the j^{th} **Reed-Muller code** *associated to $\mathbb{X}$ and denoted by $C_j(\mathbb{X})$.*

b) The minimal distance of $C_j(\mathbb{X})$ is

$$m(C_j(\mathbb{X})) = \max\{i \mid \mathbb{X} \textit{ is } (i,j)\textit{-uniform } \} + 1$$

Consequently, computing the minimal distances of the Reed-Muller codes associated to $\mathbb{X}$ is equivalent to computing the region of uniformity of $\mathbb{X}$.

3 Computing Hilbert-Kunz Functions

$K = \mathbb{F}_q$ finite field having $q = p^e$ elements

$R = K[x_0, \dots, x_n]/I$ 1-dimensional standard graded K-algebra

Definition 3.1. The function $\mathrm{HK}_R : \mathbb{N} \longrightarrow \mathbb{N}$ defined by $\mathrm{HK}_R(i) = \dim_K R/(x_0^{p^i}, \dots, x_n^{p^i})$ is called the **Hilbert-Kunz function** of R.

Proposition 3.2 (P. Monsky)
If $\dim(R) = 1$ *then there is a number* $c(R) \in \mathbb{N}$ *and a periodic function* $\varphi : \mathbb{N} \longrightarrow \mathbb{N}$ *such that* $\mathrm{HK}_R(i) = c(R) \cdot p^i + \varphi(i)$ *for all* $i >> 0$.

It is known that $c(R)$ is the multiplicity of R. Thus it can be computed.

Problems. 1) How can one compute φ? Is there a bound for the length of the period of φ?

2) How can we find $N \in \mathbb{N}$ such that the formula of the proposition holds for $i \geq N$?

Easy Reductions. 1) By computing a reduced Gröbner basis of I, we may assume that K is the field of definition of I.

2) By computing $J = H^0_{\mathfrak{m}}(R) = \{r \in R \mid \mathfrak{m}^i \cdot r = 0 \text{ for some } i \geq 0\}$, where $\mathfrak{m} = (x_0, \dots, x_n)$, we may assume that I is saturated.

3) By passing to a finite extension field of K and by performing a linear change of coordinates, we may assume that $x_0 \in R_1$ is a nonzero divisor.

4) By enlarging K if necessary, we may assume that the support of $\mathbb{X} = \mathrm{Proj}(R)$ consists of K-rational points.

Proposition 3.3 *Consider the following instructions.*

1) *If* $H^0_{\mathfrak{m}}(R) \neq 0$*, define* $M = \max\{i \in \mathbb{N} \mid (H^0_{\mathfrak{m}}(R))_i \neq 0\}$ *and replace* R *by* $R/H^0_{\mathfrak{m}}(R)$*.*
2) *Enlarge* K *to a field* $K' = F_{q^{e'}}$ *such that there is a linear nonzero divisor in* $R' = K' \otimes R$ *and the support of* $\mathbb{X} = \mathrm{Proj}(R')$ *consists of* K'*-rational points* $\{P_1, \ldots, P_s\}$*.*
3) *For* $i = 1, \ldots, s$*, compute the* **nilpotency index**

$$e_i = \min\{k \in \mathbb{N} \mid (\mathfrak{m}_{\mathbb{X},P_i})^k = 0\}$$

of $\mathbb{X}$ *at* P_i *and set* $N = \max\{e_1, \ldots, e_s, M+1\}$*.*

4) *Return the pair* (N, e') *and stop.*

This is an algorithm which computes numbers N, e' *such that*

$$\mathrm{HK}_R(i) = \mathrm{mult}(R)\, p^i + \varphi(i) \qquad \textit{whenever } p^i \geq N$$

and such that φ *is a periodic function whose period length divides* e'*.*

This algorithm has been implemented by V. Augustin. For reduced zero-dimensional schemes one can easily prove $\mathrm{HK}_R(i) = sp^i - s + 1$ for all $i \geq 0$. But for non-reduced zero-dimensional schemes there are many open questions. For instance, the analogue of the theorem of Alexander-Hirschowitz (i.e. the Hilbert-Kunz function of generically chosen double points) is not known.

Literature. 1) P. Monsky, The Hilbert-Kunz function, Math. Ann. **263** (1983), 43–39

2) M. Kreuzer, Computing Hilbert-Kunz functions of 1-dimensional graded rings, preprint 2000

3) V. Augustin, Effective computation of Hilbert-Kunz functions (in German), diplom thesis, Regensburg University 2001