On the regularity of Cactus Schemes

Daniele Taufer

Joint work with Alessandra Bernardi and Alessandro Oneto

CISPA
Helmholtz Center for Information Security

June 2021
The problem

Geometric formulation
Among the zero-dimensional schemes $Z$ apolar to a given degree-$d$ form $F$, is it true that those of minimal degree are $d$-regular?

Algebraic formulation
Does the Hilbert function of a zero-dimensional ideal $I$, which is apolar to a given degree-$d$ form $F$, stabilize in degree $d$?

\[
\begin{array}{c}
\text{codim } I_d \\
\text{deg } Z(I)
\end{array}
\]

\[d \quad D\]
1 Apolarity

2 GADs and associated schemes

3 Regularity theorem

4 Consequences

5 Work in progress
Apolarity

Setting

\[ k = \bar{k}, \; \text{char}(k) = 0, \; S = \mathbb{k}[x_0, \ldots, x_n] = \bigoplus_{d \geq 0} S_d. \]

Apolar ideal

The apolar ideal to \( F \in S_d \) is

\[ F^\perp = \{ H \in S \mid H(\delta)(F) = 0 \} \]

Example

In \( \mathbb{k}[X, Y, Z] \) we have

\[ (X^3 + X^2 Y)^\perp = \langle X^3 - 3X^2 Y, Y^2, Z \rangle. \]
Apolarity

A zero-dimensional scheme $Z$ is said to be **apolar** to $F$ if

$$I(Z) \subseteq F^\perp.$$  

Cactus schemes

The **cactus rank** of $F$ is the minimum degree of an apolar scheme of $F$. We call **cactus scheme** a scheme apolar to $F$ that computes its cactus rank.

Example

The cactus rank of $X^3 + X^2Y$ is 2, and a cactus scheme is defined by the ideal

$$\langle Y^2, Z \rangle \subsetneq (X^3 + X^2Y)^\perp.$$
1 Apolarity

2 GADs and associated schemes

3 Regularity theorem

4 Consequences

5 Work in progress
Generalized Additive Decomposition

**Generalized additive decomposition (GAD)**

Let $F \in S_d$ and let $L_1, \ldots, L_s \in S_1$ be different linear forms. A **generalized additive decomposition** (GAD) of $F$ supported at $(L_1, \ldots, L_s)$ is an expression

$$F = \sum_{i=1}^{s} L_i^{d-k_i} G_i,$$

where $0 \leq k_i \leq d$, for all $i \in \{1, \ldots, s\}$, where $L_i$ does not divide $G_i$, for each $i \in \{1, \ldots, s\}$. 
Generalized Additive Decomposition

**Example**

Let us indicate the supports with the blue color.

\[
X^3 + X^2 Y = (X)^3 \cdot 1 + (Y) \cdot X^2 \quad \checkmark
\]
\[
= (X)^3 \cdot 1 + (X)^2 \cdot Y \quad \times
\]
\[
= (X)^2 \cdot (X + Y) \quad \checkmark
\]
\[
= (X) \cdot (X^2 + XY) \quad \times
\]
\[
= (X - Y)^0 \cdot (X^3 + X^2 Y) \quad \checkmark
\]
\[
= (X + Z)^0 \cdot (X^3 + X^2 Y) \quad \checkmark
\]
Natural scheme apolar to $F$ at $L$

We associate a 0-dimensional scheme to a GAD [1, 2]:

**Natural apolar scheme**

Given a linear form $L \in S_1$, we denote the de-homogenization of $F$ with respect to $L$ by $f_L$. The affine natural scheme apolar to $F$ at $L$ is defined by

$$Z_{F,L}^a = V(f_{L}^\perp),$$

and its homogenization $Z_{F,L}$ with respect to $L$ is called the natural scheme apolar to $F$ at $L$.

**Fact [2, Corollary 4]**

$Z_{F,L}$ is apolar to $F$.  

Daniele Taufer (CISPA)
We say that the scheme

\[ Z = Z_1 \cup \ldots \cup Z_s, \quad \text{with } Z_i = Z_{L_i^{d-k_i}} L_i \]

\textbf{evinces} the GAD

\[ F = \sum_{i=1}^{s} L_i^{d-k_i} G_i. \]

The \textbf{size} of the GAD is

\[ \sum_{i=1}^{s} \deg(Z_i). \]
Scheme evincing a GAD

Example

Let us consider the (valid) GADs of $X^3 + X^2 Y$:

i) $(X)^3 \cdot 1 + (Y) \cdot X^2$

ii) $(X)^2 \cdot (X + Y)$

iii) $(X - Y)^0 \cdot (X^3 + X^2 Y)$

iv) $(X + Z)^0 \cdot (X^3 + X^2 Y)$

The schemes evincing them are

<table>
<thead>
<tr>
<th></th>
<th>Size</th>
<th>Reg</th>
</tr>
</thead>
<tbody>
<tr>
<td>i)</td>
<td>$Z_{X^3}, X \cup Z_{X^2 Y}, Y = V(\langle Y, Z \rangle \cap \langle X^3, Z \rangle) = V(\langle X^3 Y, Z \rangle)$</td>
<td>4</td>
</tr>
<tr>
<td>ii)</td>
<td>$Z_{X^2(X+Y),X} = V(\langle Y^2, Z \rangle)$</td>
<td>2</td>
</tr>
<tr>
<td>iii)</td>
<td>$Z_{X^3+X^2 Y, X-Y} = V(\langle (X + Y)^4, Z \rangle)$</td>
<td>4</td>
</tr>
<tr>
<td>iv)</td>
<td>$Z_{X^3+X^2 Y, X+Z} = V(\langle (X - Z)^2(X - 3Y - Z), Y^2 \rangle)$</td>
<td>6</td>
</tr>
</tbody>
</table>
1 Apolarity

2 GADs and associated schemes

3 Regularity theorem

4 Consequences

5 Work in progress
Regularity theorem

Regularity of schemes evincing GADs

Theorem

Let $F \in S_d$ and $Z$ be a scheme evincing one of its GADs. Then $Z$ is regular in degree $d$.

Recall: regularity in degree $d$

The Hilbert function of $I(Z)$ stabilizes to

$$\dim(\mathbb{k}(X)/I(Z))_d = \deg(Z).$$
Sketch of the proof

**Theorem**

Let $F \in S_d$ and $Z$ be a scheme evincing one of its GADs. Then $Z$ is regular in degree $d$.

**Idea of the proof**

- Local case: $Z_{L^{d-k}Q, L}$ is contained in the $k$-fat point supported at $L$.
- Merge local cases: inverse systems corresponding to different supports are linearly independent.
- To do it: read their elements as generalized eigenvectors, common to the same multiplication operators.
By [1, Theorem 3.7], the set of forms of degree $d$ with a GAD of minimal size $r$ coincides with the set of forms with cactus rank equal to $r$. Hence

**Corollary**

For every $F \in S_d$ there exists a cactus scheme of $F$ that is regular in degree $d$.

**Example**

The natural scheme apolar to $X^3 + X^2 Y$ at $X$

$$V(\langle Y^2, Z \rangle)$$

is a cactus scheme that is regular in degree 1, hence in degree $d = 3$. 
1. Apolarity

2. GADs and associated schemes

3. Regularity theorem

4. Consequences

5. Work in progress
In [3, Section 6] we presented an algorithm to recover a GAD of minimal size for $F \in S_d$, but we needed testing bases of $A = \mathbb{k}[X]/I$ of degree up to $\sim r$ (the cactus rank).

By Corollary 1, only bases with degree up to $d$ need to be tested.

**Example**

If we are dealing with a tensor in $\mathbb{k}[X, Y, Z]$ of degree $d = 4$ and rank $r = 7$, we do not need to test bases like

$$[1, Y, Z, Y^2, Y^3, Y^4, Y^5]$$

anymore.
Interpolation polynomials

Let $I$ be a zero-dimensional ideal supported at $\{P_j\}_{1 \leq j \leq s}$, namely its primary decomposition is

$$I = \bigcap_{1 \leq j \leq s} Q_j, \quad \sqrt{Q_j} = m_{P_j}.$$ 

We can always construct [4, Section 3] special interpolation polynomials $\{u_i\}_{1 \leq i \leq s}$ such that

$$\begin{cases} 
    u_i(P_j) = \delta_{i,j}, \\
    u_i^2 \equiv u_i & \in \mathbb{k}[X]/I, \\
    \sum_{i=1}^s u_i \equiv 1 & \in \mathbb{k}[X]/I.
\end{cases}$$

By construction, the degree of these $u_i$’s may be assumed to be lower than the regularity of $I$, which in our setting is bounded by $d$. 

1 Apolarity
2 GADs and associated schemes
3 Regularity theorem
4 Consequences
5 Work in progress
## Non-redundant schemes

A scheme $Z$ apolar to $F$ is called **non-redundant** if there are no proper subschemes $Z' \subsetneq Z$ apolar to $F$.

Notice: cactus implies non-redundancy.

## Claim

Every non-redundant scheme $Z$ apolar to $F \in S_d$ is regular in degree $d$.

Idea of the proof: given $I \subseteq F^\perp$, we produce $I \subseteq J \subseteq F^\perp$ that evinces a GAD of $F$. 

---

**Work in progress**

**On the regularity of every non-redundant scheme**

---

Daniele Taufer (CISPA)

On the regularity of Cactus Schemes

June 2021 17 / 19
An extended example

Let us consider

\[ F = X^3 + 3X^2Y + 3X^2Z + 3XY^2 + 12XYZ + Y^3 + 3Y^2Z \in S_3, \]

and

\[
I = \langle Y, Z \rangle^3 \cap \langle X - Y, Z \rangle^2 \\
= \langle X^2Y^3 - 2XY^4 + Y^5, XY^2Z - Y^3Z, YZ^2, Z^3 \rangle.
\]

We have

\[ I \subseteq F^\perp. \]

We want

\[ I \subseteq J \subseteq F^\perp \text{ evincing a GAD of } F. \]
On the regularity of every non-redundant scheme

An extended example

We fill the Hankel matrix $H_F$ of $F$ in order to have $I \subseteq \ker H_F$:

$$
\begin{bmatrix}
1 & 1 & 1 & 1 & 2 & 0 & 1 & 1 & 0 & 0 \\
1 & 1 & 2 & 1 & 1 & 0 & h_1 & h_2 & h_3 & h_4 \\
1 & 2 & 0 & 1 & 0 & 0 & h_2 & h_3 & h_4 & h_5 \\
1 & 1 & 1 & h_1 & h_2 & h_3 & h_6 & h_7 & h_8 & h_9 \\
2 & 1 & 0 & h_2 & h_3 & h_4 & h_7 & h_8 & h_9 & h_{10} \\
0 & 0 & 0 & h_3 & h_4 & h_5 & h_8 & h_9 & h_{10} & h_{11} \\
1 & h_1 & h_2 & h_6 & h_7 & h_8 & h_{12} & h_{13} & h_{14} & h_{15} \\
1 & h_2 & h_3 & h_7 & h_8 & h_9 & h_{13} & h_{14} & h_{15} & h_{16} \\
0 & h_3 & h_4 & h_8 & h_9 & h_{10} & h_{14} & h_{15} & h_{16} & h_{17} \\
0 & h_4 & h_5 & h_9 & h_{10} & h_{11} & h_{15} & h_{16} & h_{17} & h_{18}
\end{bmatrix}
$$
On the regularity of every non-redundant scheme

An extended example

We fill the Hankel matrix $H_F$ of $F$ in order to have $I \subseteq \ker H_F$:

$$
\begin{bmatrix}
1 & 1 & 1 & 1 & 2 & 0 & 1 & 1 & 0 & 0 \\
1 & 1 & 2 & 1 & 1 & 0 & \frac{h_{57}+7}{8} & 1 & 0 & 0 \\
1 & 2 & 0 & 1 & 0 & 0 & 1 & 0 & 0 & 0 \\
1 & 1 & 1 & \frac{h_{57}+7}{8} & 1 & 0 & \frac{h_{57}+3}{4} & 1 & 0 & 0 \\
2 & 1 & 0 & 1 & 0 & 0 & 1 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
1 & \frac{h_{57}+7}{8} & 1 & 0 & 1 & 0 & \frac{3h_{57}+5}{8} & 1 & 0 & 0 \\
1 & 1 & 0 & 1 & 0 & 0 & 1 & 0 & 0 & \frac{h_{57}+3}{4} \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & h_{57}+\frac{3}{4} & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & h_{57}+\frac{3}{4} & 0 & 0 \\
\end{bmatrix}
$$
On the regularity of every non-redundant scheme

An extended example

We fill the Hankel matrix $H_F$ of $F$ in order to have $I \subseteq \ker H_F$:

$$h_{57} = 1$$

$$H_G = \begin{bmatrix}
1 & 1 & 1 & 1 & 2 & 0 & 1 & 1 & 0 & 0 \\
1 & 1 & 2 & 1 & 1 & 0 & 1 & 1 & 0 & 0 \\
1 & 2 & 0 & 1 & 0 & 0 & 1 & 0 & 0 & 0 \\
1 & 1 & 1 & 1 & 1 & 0 & 1 & 1 & 0 & 0 \\
2 & 1 & 0 & 1 & 0 & 0 & 1 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
1 & 1 & 1 & 0 & 1 & 0 & 1 & 1 & 0 & 0 \\
1 & 1 & 1 & 0 & 0 & 1 & 0 & 0 & 0 & 1 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\
\end{bmatrix}$$
On the regularity of every non-redundant scheme

An extended example

The kernel of this matrix is

\[ J' = \langle XY^2 - Y^3, Z^2 \rangle \supseteq I. \]

\( V(J') \) evinces a GAD for an extension \( G \) of \( F \):

\[ G = \frac{1}{120} (30X^4YZ + (X + Y)^5(X + Y + 6Z)). \]

We obtain by derivation \( \partial_X^3 G = F \) a GAD of \( F \), which is evinced by a scheme defined by \( V(J) \) for some \( J \supseteq J' \) (in our example: \( J = J' \)):

\[ V(J) \) evinces \( F = 6XYZ + (X + Y)^2(X + Y + 3Z). \)

