Primary decomposition - zero-dimensional case

Let $\mathbb{K}$ be an algebraically closed field with $\operatorname{char}(\mathbb{K}) = 0$. $\bar{x} = \{x_1, \dots, x_n\}$

Remark: today we will make the simplifying assumption that $\mathbb{K}$ is algebraically closed. In general we don't want to make this assumption.

Input: $I \subseteq \mathbb{K}[\bar{x}]$ ideal s.t. $\dim I = 0$
Output: $Q_1, \dots, Q_s$ s.t. $I = \bigcap_{i=1}^{s} Q_i$ irredundant primary decomposition

In the zero dimensional case we will see that primary decomposition will reduce to univariate factorization.

When $\dim I = 0$, then every $\mathfrak{P} \in \operatorname{Ass}(I)$ is a maximal ideal ($\therefore$ I has no embedded primes).
By Hilbert's Nullstellensatz, we know that every maximal ideal is of the form $(x_1 - \alpha_1, \dots, x_n - \alpha_n)$ for some $\bar{\alpha} \in \mathbb{K}^n$.
However our ideal I is the intersection of many primary ideals with maximal primes. So we need to be able to distinguish them.
We will do it by putting our ideal in "general position"

Definition 1 (general position):
$I \subset \mathbb{K}[\bar{x}]$ with $\dim I = 0$ is in general position w.r.t. Lex order if $\forall\, \mathfrak{P} \neq \mathfrak{Q} \in \operatorname{Ass}(I) \Rightarrow$ $\mathfrak{P} \cap \mathbb{K}[x_n] \neq \mathfrak{Q} \cap \mathbb{K}[x_n]$.

Proposition 2: Let $I \subset \mathbb{K}[\bar{x}]$ with $\dim I = 0$. There is a non-empty open set $U \subset \mathbb{K}^{n-1}$ s.t. for all $\bar{a} := (a_1, \dots, a_{n-1}) \in U$, the coordinate change $\varphi_{\bar{a}} : \mathbb{K}[\bar{x}] \to \mathbb{K}[\bar{x}]$ given by $\varphi_{\bar{a}}(x_i) = x_i$ $i \in [n-1]$ and $\varphi_{\bar{a}}(x_n) = x_n + \sum_{i=1}^{n-1} a_i x_i$ has the property that

$\varphi_{\bar{a}}(I)$ is in general position w.r.t. Lex.

Proof: Let $\mathfrak{P} = (x_1 - \alpha_1, \dots, x_n - \alpha_n)$ and $\mathfrak{Q} = (x_1 - \beta_1, \dots, x_n - \beta_n)$ be s.t. $\mathfrak{P}, \mathfrak{Q} \in \operatorname{Ass}(I)$ and $\mathfrak{P} \neq \mathfrak{Q}$. Hence $\bar{\alpha} \neq \bar{\beta}$. Note that
$\varphi_{\bar{a}}(\mathfrak{P}) = (x_1 - \alpha_1, \dots, x_{n-1} - \alpha_{n-1}, x_n + \sum_{i=1}^{n-1} a_i \alpha_i - \alpha_n)$
and similarly
$\varphi_{\bar{a}}(\mathfrak{Q}) = (x_1 - \beta_1, \dots, x_{n-1} - \beta_{n-1}, x_n + \sum_{i=1}^{n-1} a_i \beta_i - \beta_n)$
Thus, so long as

$$\sum_{i=1}^{n-1} a_i (\alpha_i - \beta_i) \neq \alpha_n - \beta_n \qquad (*)$$

we will have that $\varphi_{\bar{a}}(\mathfrak{P}) \cap \mathbb{K}[x_n] \neq \varphi_{\bar{a}}(\mathfrak{Q}) \cap \mathbb{K}[x_n]$.
Since $\bar{\alpha} \neq \bar{\beta}$ we have $(*)$ is the non-vanishing of a nonzero polynomial $\therefore$ an open condition.
The result now follows as the intersection of finitely many open sets is open. $\square$

Proposition 3: Let $I \subset \mathbb{K}[\bar{x}]$ with $\dim I = 0$ and let $(g) = I \cap \mathbb{K}[x_n]$ be s.t. $g = \prod_{i=1}^{s} (x_n - \alpha_i)^{\nu_i}$ with $\alpha_i \neq \alpha_j$ for $i \neq j \in [s]$. Then
① $I = \bigcap_{i=1}^{s} (I, (x_n - \alpha_i)^{\nu_i})$

② If I is in general position w.r.t. Lex order then $(I, (x_n - \alpha_i)^{\nu_i})$ is a primary ideal for all $i \in [s]$.

Proof: ① Since $I \subset (I, (x_n - \alpha_i)^{\nu_i})$ we have $I \subseteq \bigcap_{i=1}^{s} (I, (x_n - \alpha_i)^{\nu_i})$. Let $g_i := g/(x_n - \alpha_i)^{\nu_i}$ for $i \in [s]$. Since $\gcd(g_1, \dots, g_s) = 1$, $\exists\, \bar{b} \in \mathbb{K}[x_n]^s$ s.t. $1 = \sum_{i=1}^{s} b_i g_i$. Let $f \in \bigcap_{i=1}^{s} (I, (x_n - \alpha_i)^{\nu_i})$.

Hence $\exists\, f_i, h_i \in \mathbb{K}[\bar{x}]$ s.t. $f = f_i + h_i (x_n - \alpha_i)^{\nu_i}$ and $f_i \in I$, $\forall\, i \in [s]$. Thus
$1 \cdot f = \sum_{i=1}^{s} b_i g_i f = \sum_{i=1}^{s} \left(b_i f_i + h_i g_i (x_n - \alpha_i)^{\nu_i}\right) =$
$= \left(\sum_{i=1}^{s} b_i f_i\right) + g \sum_{i=1}^{s} h_i \in I$.

② First note that $(I, (x_n - \alpha_i)^{\nu_i}) \neq \mathbb{K}[\bar{x}]$ since $1 \in (I, (x_n - \alpha_i)^{\nu_i}) \Rightarrow \exists\, f \in I, h \in \mathbb{K}[\bar{x}]$ s.t. $1 = f + h(x_n - \alpha_i)^{\nu_i}$
$\Rightarrow g_i = g_i f + h g \in I$ which contradicts $I \cap \mathbb{K}[x_n] = (g)$.
Since $I \subset (I, (x_n - \alpha_i)^{\nu_i})$ we have that $\mathfrak{P} \in \operatorname{Ass}(I, (x_n - \alpha_i)^{\nu_i})$
$\Rightarrow \exists\, \mathfrak{Q} \in \operatorname{Ass}(I)$ s.t. $\mathfrak{Q} \subset \mathfrak{P}$. Since $\mathfrak{Q}$ max'l (as $\dim I = 0$) we must have $\mathfrak{Q} = \mathfrak{P}$.
Thus, we have also that $\operatorname{Ass}((I, (x_n - \alpha_i)^{\nu_i})) \subset \operatorname{Ass}(I)$.
Since associated primes of zero dim'l ideals are maximal let $\{\mathfrak{P}_1, \dots, \mathfrak{P}_\ell\} = \operatorname{Ass}(I)$. Then $\mathfrak{P}_i = (x_j - \alpha_{ij})_{j=1}^{n}$ $\forall i \in \ell$.
I in general position $\Rightarrow \alpha_{in} \neq \alpha_{jn}$ $\forall\, i \neq j \in [\ell] \Rightarrow$ $\ell = s$ and we can take $\alpha_{in} = \alpha_i$ $\forall\, i \in [s]$.
By the above note that $\emptyset \neq \operatorname{Ass}(I, (x_n - \alpha_i)^{\nu_i}) \subset \operatorname{Ass}(I)$ and we also have that $\mathfrak{P}_i$ is the only associated prime of I that contains $(I, (x_n - \alpha_i)^{\nu_i})$ $\therefore$
$\operatorname{Ass}(I, (x_n - \alpha_i)^{\nu_i}) = \{\mathfrak{P}_i\} \Rightarrow$ primary. $\square$

The above propositions already give us a randomized algorithm to obtain a primary decomposition of a zero-dimensional ideal, as a random map will put our input ideal into general position.
(here I am assuming we have a factoring algorithm over $\mathbb{K}[y]$, i.e. univariate polynomials over $\mathbb{K}$).
To make this a zero-error probabilistic algorithm, we need a way to verify that the ideals $(I, (x_n - \alpha_i)^{\nu_i})$ that we obtain are actually primary.
But this verification step for us is very simple (when $\mathbb{K}$ is algebraically closed) by the following proposition:

Proposition 4: $I \subset \mathbb{K}[\bar{x}]$ with $\dim I = 0$ is primary $\Leftrightarrow$ $I \cap \mathbb{K}[x_i] = ((x_i - \alpha_i)^{\nu_i})$ for some $\alpha_i \in \mathbb{K}$ and $\nu_i \in \mathbb{N}$.