1 Lacunary/Sparsepoly Polynomials

Let $P$ be a field and $f(x) \in P[x]$ of degree $n$, write 
$$ f(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_0. $$ 
with $a_k \neq 0, \ldots, a_0 \in P \setminus \{0\}$, and $e_1, \ldots, e_k \in \mathbb{Z}$, and $e_{k+1} \cdots e_{n-1} < e_0$.

This corresponds to the sparse representation of $f(x)$ by a list of nonzero coefficient-exponent pairs $(a_k, e_k, \ldots, a_0)$. 

Size is $\sum |a_i| (e_i + 1)$.

• Can be exponentially smaller than the dense size.

• This representation is the default in Maple, Mathematica, etc.

2 Sparse Shift Interpolation

Definition (Sparse Shifts, If $f(x)$ has at most $t$ nonzero terms in the shifted power basis $1, x, (x-1), \ldots, x^{t-1}$, for some $t \in P$, then we say $x$ is a $t$-sparse shift for $f(x)$.

Theorem (Lasku & Samuelson [9], $t \leq \ell$), there is at most one $t$-sparse shift for a given polynomial $f(x) \in P[x]$.

Algorithm to find sparse shift when input is given as $[8, 5]$.

Goal: an algorithm to find the sparsest shift of $f(x)$ given a black box for evaluation, with complexity polynomial in the size of the sparsest shift.

We have a solution to a particular instance of this problem: Let $f(x) \in \mathbb{Z}[x]$, and suppose we are given a black box which takes $f(x) \in \mathbb{Z}[x]$ and a prime $p$, and returns $f(x) \bmod p$.

3 Polynomial Decomposition

Functional Decomposition Problem (minimise, simple): Given $f(x) \in P[x]$, find $g(x), h(x) \in P[x]$ with $\deg g + \deg h \leq 2$ and $f(x) = g(x) h(x)$.

Well-studied problem when input is given in the dense representation. The usual approach is to find $h(x)$ first, then use $h(x)$ to find $g(x)$.

4 Future Work

• Using a sparse shift interpolation algorithm to find $g(x)$ of high degree given $h(x)$.

• Extending sparse shift interpolation algorithm to work over fields other than $\mathbb{Z}[x]$.

• Eliminating the dependency of the algorithm for finding high-degree $h(x)$ on any conjectures.

• Removing the output-sensitivity of the runtime (i.e., proving that $h(x)$ and $g(x)$ are always sparse when $f(x)$ is sparse) — relates to [11] and many others.

• Finding an algorithm to certify valid right composition factor $h(x)$ of high degree. Note that an algorithm to perform a polynomial divisibility check would solve this.

References


