

1106-VQ-2117 **Joshua E Hill*** (hillje@uci.edu). *On Calculating the Cardinality of the Value Set of a Polynomial.*

We prove a combinatorial identity that relates the size of the value set of a map with the sizes of various iterated fiber products by this map. This identity is then used as the basis for several algorithms that calculate the size of the value set of a polynomial for a broad class of algebraic spaces, most generally an algorithm to calculate the size of the value set of a suitably well-behaved morphism between “nice” affine varieties defined over a finite field. These algorithms specialize to the case of calculating the size of the value set of a polynomial, viewed as a map between finite fields. These algorithms operate in deterministic polynomial time for fixed input polynomials (thus a fixed number of variables and polynomial degree), so long as the characteristic of the field grows suitably slowly as compared to the other parameters.

These value set cardinality calculation algorithms extend to amortized cost algorithms that offer dramatic computational complexity advantages, when the computational cost is amortized over all the results produced. The last of these amortized algorithms partially answers a conjecture of Wan, as it operates in time that is polynomial in $\log q$ per value set cardinality calculated. (Received September 15, 2014)