Polynomials Modulo Composite Numbers: Ax-Katz type theorems for the structure of their solution sets

Robert Surówka and Kenneth W. Regan

Department of CSE, University at Buffalo, Amherst, NY 14260 USA
{robertlu,regan}@buffalo.edu

August 19, 2014

Abstract

Marshall and Ramage extended a theorem of Ax from finite fields to finite principal rings, including the rings \( \mathbb{Z}_m \) with \( m \) composite. We extend their result further by showing additional symmetric structure of the solution spaces. Additionally, for the restricted case of \( \mathbb{Z}_{2^r} \) and polynomials of degree up to 2, we demonstrate even more complex symmetries. Finally, we present experimental results showing solution spaces of polynomials for chosen rings and degrees, to facilitate further hypothesis formulation in this area. Polynomials modulo composites are the focus of some computational complexity lower bound frontiers, while those modulo \( 2^r \) arise in the simulation of quantum circuits. We give some prospective applications of this line of inquiry.

1 Introduction

Let \( P \) be an \( n \)-variable polynomial \( P : \mathbb{F}_p^n \to \mathbb{F}_p \) over a finite field \( \mathbb{F}_p \). The Chevalley-Warning theorem \([13, 30]\) states that if \( n > \deg P \geq 1 \) then \( p \) divides \( \#0_P \) (where \( \#0_P \) denotes the number of zeros of \( P \) in \( \mathbb{F}_p \)). Ax \([4]\), using an idea of Dwork \([16]\), greatly improved this result, to state that

\[
\#0_P \text{ is a multiple of } p^r\left(\frac{n}{d}\right)-1,
\]

where \( d \) is the degree of \( P \). This result was extended to systems \( P \) of \( q \)-many polynomials \( P_i : \mathbb{F}_p^n \to \mathbb{F}_p \) with respective degrees \( d_i \). Letting \( \#0_P \) be the number of their common zeroes, Katz \([22]\) proved that

\[
\#0_P \text{ is a multiple of } p^r\left[\frac{n}{\sum d_i}\right]-1.
\]

For a single polynomial this is equivalent to the initial result by Ax. Additionally, the Ax-Katz theorem is known to be optimal, in regard to the gcd of the cardinalities of the solution sets.

The result we directly build on was obtained by Marshall and Ramage \([23]\). For a polynomial \( P \) over a ring \( \mathbb{Z}_m \) (or even for any finite, principal ring), where \( m = p_1^{r_1}p_2^{r_2} \ldots p_k^{r_k} \) and all \( p_1, p_2, \ldots, p_k \) are different primes, they proved that

\[
\#0_P \text{ is a multiple of } \prod_{i,r_i=1} p_i^{\left[\frac{n}{d_i}\right]} \prod_{i,r_i>1} p_i^{\left[\frac{n}{d_i-1}\right]}.
\]

The above was extended by Daniel Katz \([21]\) to find the gcd of the numbers of solutions of sets of \( q \)-many polynomials in \( n \) variables. There had been a lot of additional work done in the area of properties of polynomial solution spaces, especially focused and building from the Ax-Katz theorem, which is by far the most well known.
One of the popular routes was simplifying that theorem’s proof. First was an ‘elementary’ proof by Wan [29], later made especially simple for prime fields [30]. Hou showed how to obtain the Ax-Katz theorem by direct deduction from Ax’s original theorem [20]. A proof requiring probably the least number-theoretic background was presented by Wilson [32]. Another results include improvements when the degrees of all variables in monomials are powers of the characteristic of the field (p-weighted degree) [24, 25, 12], specializations for so-called general diagonal equations [10, 11], partial results when variables with high degrees are ignored or there are isolated variables [8, 9, 12], divisibility for exponential sums [3, 25], situations when solutions are specific subspaces of the domain [19], and many more instances. Apart from the interest in the divisibility of the numbers of solutions, there is also a research in establishing how large such numbers need to be, when they are non-zero. First such a result is Warning’s Second Theorem [30], followed by results of Schanuel [27], Brink [6] and, very recently, Clark, Forrow and Schmitt [14]. This last reference improves the bound and also explores the situation when variables of polynomials are bounded to subsets of the domain, notably the Boolean cube \( \{0,1\}^n \).

2 Statement of the results

Our first result applies the proof technique of Marshall and Ramage [23] to show an additional symmetry in the solution space. Taking \( #k_Q \) to be a number of solutions of \( Q - k \) we prove that:

**Theorem 1.** For any polynomial \( Q \) of \( n \geq 2 \) variables \( x \) of degree \( d \) over \( \mathbb{Z}_m \), where \( m = p_1^{n_1} p_2^{n_2} \ldots p_v^{n_v} \) and all \( p_1, p_2, \ldots, p_v \) are different primes, and any integers \( k, w_1, w_2, \ldots, w_v, q_1, q_2, \ldots, q_v \), where \( q_i \leq n \), it holds that:

\[
\sum_{i_1=0}^{p_1^{n_1}-1} \sum_{i_2=0}^{p_2^{n_2}-1} \cdots \sum_{i_v=0}^{p_v^{n_v}-1} \# \left( k + \sum_{j=1}^{v} w_j m \frac{p_i}{p_j} \right) \text{ is a multiple of } \prod_{i, r_i=1}^{v} p_i^{\left[ \frac{x_i}{r_i} \right] + q_i - 1} \prod_{i, r_i > 1}^{v} p_i^{\left[ \frac{x_i}{r_i} \right] + q_i - 1}.
\]

Using another approach, we obtain a result demonstrating even more symmetries, but restricting both the degree of the polynomial and the ring characteristic to \( 2 \).

**Theorem 2.** (Main Theorem) For any polynomial \( Q \) of \( n \geq 3 \) variables \( (x, z) \) over \( \mathbb{Z}_{2^r} \) of degree up to \( 2 \), any integers \( q, v \leq r \) and \( k, w, g, u \) and any linear polynomial \( T(x) \), it holds that:

\[
\sum_{i=0}^{2^v-1} \sum_{j=0}^{2^v-1} \# (k+w2^{r-q}i+g2^{r-v}j)_{Q,z=T(x)+u2^{r-v}z} \text{ is a multiple of } 2^{\left[ \frac{r(n-1)+\min(2r,v)}{2} \right] + q-1}.
\]

The properties below easily follow, as we will show in section 4.

**Corollary 1.** For any polynomial \( Q \) of \( n \geq 3 \) variables \( (x, z) \) over \( \mathbb{Z}_{2^r} \) of degree up to \( 2 \), and any integers \( q,v \leq r \) and \( k, w, g, l \), it holds that:

(a) \[
\sum_{j=0}^{2^r-1} \# k_{Q,z=l+g2^{r-v}z} \text{ is a multiple of } 2^{\left[ \frac{r(n-1)+\min(2r,v)}{2} \right] - 1}, \quad n \geq 3
\]

(b) \[
\sum_{i=0}^{2^q-1} \sum_{j=0}^{2^v-1} \# (k+w2^{r-q}i)_{Q,z=l+g2^{r-v}z} \text{ is a multiple of } 2^{\left[ \frac{r(n-1)+\min(2r,v)}{2} \right] + q-1}, \quad n \geq 3
\]

(c) \[
\sum_{j=0}^{2^v-1} \# (k+w2^{r-q}j)_{Q,z=l+g2^{r-v}z} \text{ is a multiple of } 2^{\left[ \frac{r(n-1)+\min(2r,v)}{2} \right] - 1}, \quad n \geq 3.
\]

Part (a) says that when one variable is limited to a coset of an ideal it only moderately decreases the divisibility—while if the coset is at least half of the ring, the divisibility does not deteriorate at all. Parts (b) and (c), and Theorem 2 overall, show that properties from Theorem 1 and point (c) add the same degree of divisibility even when both properties are present. This works even in somewhat more general settings.

We should note here, that the proof technique of Marshall and Ramage [23] easily allows to prove point (a) of the above corollary for polynomial of unbounded degree and for \( \mathbb{Z}_m \), but only when \( v = r - 1 \).
3 Proof of Theorem 1

Theorem 1. For any polynomial $Q$ of $n \geq 2$ variables $\mathbf{x}$ over $\mathbb{Z}_m$, where $m = p_1^{\alpha_1}p_2^{\alpha_2} \ldots p_v^{\alpha_v}$ and all $p_1, p_2, \ldots, p_v$ are different primes, and any integers $k, w_1, w_2, \ldots, w_e, q_1, q_2, \ldots, q_e$, where $q_i \leq r_i$ there is an integer $T$ such that:

$$\sum_{i_1=0}^{p_1^{\alpha_1}-1} \sum_{i_2=0}^{p_2^{\alpha_2}-1} \cdots \sum_{i_v=0}^{p_v^{\alpha_v}-1} \sum_{j=1}^{v} w_j m_{i_j} \cdot (k + \sum_{j=1}^{v} w_j m_{i_j}) = T \prod_{i, r_i=1}^{p_1^{\alpha_1}} p_i^{\frac{q_i}{r_i}} \prod_{i, r_i>1}^{p_1^{\alpha_1}} p_i^{\frac{r_i-1}{r_i}}.$$

Proof. We rely on the proof technique of [23]. Let us start by proving the hypothesis for a ring $\mathbb{Z}_{p^r}$, where $p$ is prime. If $r = 1$ we wish to prove that

$$\sum_{i=0}^{p^r-1} \#(k+w_i) = Tp^\frac{q_i}{r_i}.$$

and it trivially follows from the Ax’s theorem. We take now $r \geq 2$, for which we intend to prove

$$\sum_{i=0}^{p^r-1} \#(k+w_i) = Tp^{\frac{q_i}{r_i}+q-1}.$$

Consider

$$C = \sum_{i=0}^{p^r-1} \#(k+w_i) = \sum_{i=0}^{p^r-1} \#(w_i)$$

where $U(x) = Q(x) - k$,

$$= \sum_{i=0}^{p^r-1} \#(p^{i-q})u$$

where $u$ is the order of $w$ (i.e. biggest power of $p$ dividing $w$, but $u \leq r$). Let $e = \max(q - w, 0)$ and let

$$C' = \sum_{i=0}^{p^r-1} \#(p^{i-q})u.$$

We need now to prove that $C'$ is a multiple of $p^{\frac{q_i}{r_i}+q-1}$. Note that if $e = r$ the result is trivial, therefore we assume $e < r$. Additionally, if $e = 0$, the result instantly reduces to the theorem by Marshall and Ramage [23]. This allows us to take $0 < e < r$. Let

$$H(x, y) = U(x) + y.$$

Then

$$C' = \sum_{i=0}^{p^r-1} \#0_{H, y=p^{i-q}}$$

because for any assignment to $x$ that makes $U(x)$ have order at least $r - e$, there is exactly one assignment to $y$ that evaluates $H$ to 0. Let $(x'_1, x'_2, \ldots, x'_n, y')$ be a solution of $H$ over $\mathbb{Z}_{p^r}$. Let us consider assignments to $H$ of the pattern

$$H(x'_1 + px_1, x'_2 + px_2, \ldots, x'_n + px_n, y' + p^{r-e}y),$$

which then has a form

$$pG_1 + p^2G_2 + \ldots + p^dG_d + p^{r-e}$$

where $G_i$ are homogeneous functions of degree $i$ in variables $x$. Thus we wish to count the number of zeroes of

$$G = G_1 + pG_2 + \ldots + p^{d-1}G_d + p^{r-e-1}y$$
over $\mathbb{Z}_{p^r-1}$, where additionally $y \in \mathbb{Z}_{p^e}$ (i.e. $0 \leq y < p^e$). First let us consider $r = 2$. Then $e = 1$, and from direct use of the Ax’s theorem on $G$, we obtain divisibility of solutions number by $p^n$ (note that $G$ in this case is linear). Let us take now $r \geq 3$. If any of the variables $x_1, \ldots, x_n$ is multiplied by a unit in $G_1$, let $t$ be one of these variables. If not, then if $r - e - 1 = 0$ let $t = y$. If $t$ was picked to be one of the variables, let us notice that for any assignment to all other variables in $G$, there is precisely one assignment to $t$ that solves $G$ (via the main Lemma of [23] if $t \neq y$). Hence $G$ has $p^{(r-1)(n-1)+e}$ solutions. Let us compare this exponent with our hypothesis (we can omit the ceiling function, since the left-hand side is integer):

$$
(r - 1)(n - 1) + e \geq \frac{rn}{2} + e - 1
$$

$$
2rn - 2r - 2n + 2e + 2 \geq rn + 2e - 2
$$

$$
2rn - 2r - 2n + 4 \geq 0 \iff (r - 2)(n - 2) \geq 0,
$$

which is always true under the theorem’s assumptions. Let us assume now that it was impossible to pick $t$, i.e. all coefficients in $G_1$ are divisible by $p$ and $r - e - 1 \geq 1$. We take $G_1 = pG'_1$ and write that

$$
G' = G'_1 + G_2 + \ldots + p^{d-2}G_d + p^{r-e-2}y.
$$

The number of zeroes of $G$ over $\mathbb{Z}_{p^r-1}$, with constraint on $y$ as earlier, equals the number of zeroes of $G'$ over $\mathbb{Z}_{p^r-2}$ multiplied by $p^n$, with unchanged constraint on $y$. By induction, or by the Ax’s result if $r = 3$, we obtain that the number of zeroes of $G'$, under the aforementioned settings, is divisible by $p^{\lceil \frac{(r-2)n}{2} \rceil + e - 1}$, which multiplied by $p^n$ gives the desired divisibility.

This analysis extends to all the rings $\mathbb{Z}_m$ via the decomposition of the ring $\mathbb{Z}_m$ into its local rings, in the same way as applied by Marshall and Ramage [23]. Equivalently, an argument using a simple application of Chinese remaindering can be employed.

\[\Box\]

4 Discussion of proof of Theorem 2

We prove this theorem by induction on the number of variables. We state the base case and the induction step of Theorem 2 separately. Curiously the base case $n = 3$ has by far the longer proof, yet while working on it we additionally prove several lemmas of independent interest. We present both proofs in section 7.

Theorem 2. (Base case)

For any polynomial $Q$ of 3 variables $(x, y, z)$ over $\mathbb{Z}_{2r}$ of degree up to 2, any integers $q, v \leq r$ and $k, w, g, u$ and any linear polynomial $T(x, y)$, there is an integer $T'$ such that:

$$
\sum_{i=0}^{2^r-1} \sum_{j=0}^{2^r-1} \#(k + w 2^{r-q} i + g 2^{r-v} j)_{Q, z = T(x,y) + u 2^{r-v}} = T 2^{r + \lceil \min(2^{r-q}) \rceil + q - 1}
$$

Theorem 2. (General induction step)

Let any quadratic polynomial $Q$ of $n \geq 4$ variables $(x, z)$ over $\mathbb{Z}_{2r}$, and any integers $q, v \leq r$ and $k, w, g, u$, and any linear polynomial $T(x)$ be given. Suppose that for any $Q'$ of $n - 1$ variables $(x', z')$, any $q', v' \leq r$ and $k', w', g', u'$, and any linear polynomial $T'(x')$ it holds that:

$$
\sum_{i=0}^{2^{k'}-1} \sum_{j=0}^{2^{k'}-1} \#(k' + w' 2^{r-q'} i + g' 2^{r-v'} j)_{Q', z' = T'(x') + u' 2^{r-v'} j} = T' 2^{r + \lceil \min(2^{r-q'}) \rceil + q' - 1}
$$

for certain integer $T'$. Then there is an integer $T$ such that

$$
\sum_{i=0}^{2^{k}-1} \sum_{j=0}^{2^{k}-1} \#(k + w 2^{r-q} i + g 2^{r-v} j)_{Q, z = T(x) + u 2^{r-v}} = T 2^{r + \lceil \min(2^{r-q}) \rceil + q - 1}.
$$
We apply the induction hypothesis for \( n - 1 \) where \( z' \) is a different variable from the \( z \) in the goal statement for \( n \). In particular \( z' \) becomes the variable in \( x \) whose coefficient in a certain linear functional inside of \( Q \) has the least order.

In the general induction step we show that if \( Q \) has no term of type \( z^2 \) then for it the theorem holds basing on induction hypothesis for \( n - 1 \) variables. Then we prove that adding the square term for \( z \) does not change the divisibility lower bound.

The form with two summation signs is very general, but we found that by our approach of inducting on \( n \) even obtaining a simple statement about the divisibility of \( \#0_Q \) requires them, else our induction does not close. The following corollary indicates statements one can obtain by substituting for the more general quantities.

**Corollary 1.** For any polynomial \( Q \) of \( n \) variables \((x, z)\) over \( \mathbb{Z}_2^r \) of degree up to 2, and any integers \( q, v \leq r \) and \( k, w, g, l \), it holds that:

\[
a) \sum_{j=0}^{2^v-1} \#k_{Q,z=\ell+g2^{r-v}j} = T_a 2^{\left\lfloor \frac{r(n-1) + \min(2v, r)}{2} \right\rfloor} - 1, \quad n \geq 3
\]

\[
b) \sum_{i=0}^{2^v-1} \sum_{j=0}^{2^{v-1}-1} \#(k+w2^{r-q}i)_{Q,z=\ell+g2^{r-v}j} = T_b 2^{\left\lfloor \frac{r(n-1) + \min(2v, r)}{2} \right\rfloor} + q - 1, \quad n \geq 3
\]

\[
c) \sum_{j=0}^{2^v-1} \#(k+w2^{r-q}j)_{Q,z=\ell+g2^{r-v}j} = T_c 2^{\left\lfloor \frac{r(n-1) + \min(2v, r)}{2} \right\rfloor} - 1, \quad n \geq 3
\]

for certain integers \( T_a, T_b, T_c \).

**Proof.** All above are special cases of Theorem 2:

a) Take \( q = 0, g = 0 \) and \( T(x) = l \).

b) Take \( g = 0 \) and \( T(x) = l \).

c) Take \( q = 0 \) and \( T(x) = l \).

\( \square \)

## 5 Experiments

Before we were able to get a feel of the behaviour of the polynomial solutions over rings, in order to formulate our theorem’s statements, we had to see first some examples. Then we were able to extrapolate from them the general properties. In this chapter we present sample computer programs we wrote and some results we obtained, which allowed us to probe this area. Those programs are extremely simple, yet they were only a mundane means for the general formulations of the properties. We present their actual Java code instead of a pseudocode, so that anyone interested can directly copy and run them himself, possibly with different parameters than the ones presented here. The most basic version of the programs we run is presented in the form of the code 1. Variables \( \text{ring} \) and \( \text{vars\_num} \) are set to the size of the ring and the number of variables of the polynomial respectively. The program outputs, for each possible number of solutions, how many polynomials of the given number of variables over the given ring (and with degree up to 2), have that many solutions. For example “0: 80”, means there are 80 polynomials that are unsolvable, whereas “3: 702” means there are 702 polynomials having 3 solutions. The code iterates over all possible polynomials, by iterating over all possible coefficients of the terms. For each such polynomial, the code iterates over all possible assignments to the polynomial’s variables, and records what the polynomial evaluates to. All those results are combined to produce the final output.
public class Solutions {

    public static boolean next(int[] arr, int ring) {
        for (int index = arr.length - 1; index >= 0; --index) {
            if (arr[index] < ring - 1) {
                ++arr[index];
                return true;
            } else {
                arr[index] = 0;
            }
        }
        return false;
    }

    public static void main(String[] args) {
        int ring = 3;
        int vars_num = 3;
        int coef_num = vars_num + (vars_num * (vars_num + 1)) / 2;
        int[] coefs = new int[coef_num];
        int[] vars = new int[vars_num];
        long[] out = new long[(int) Math.pow(ring, vars_num) + 1];
        int[] ringout = new int[ring];
        coefs[coefs.length - 1] = -1;
        while (next(coefs, ring)) {
            for (int i = 0; i < ring; ++i) {
                ringout[i] = 0;
            }
            for (int i = 0; i < vars_num; ++i) {
                vars[i] = 0;
            }
            vars[vars.length - 1] = -1;
            while (next(vars, ring)) {
                int result = 0;
                for (int i = 0; i < vars_num; ++i) {
                    result += coefs[i] * vars[i];
                }
                int off = vars_num;
                for (int i = 0; i < vars_num; ++i) {
                    for (int j = i; j < vars_num; ++j) {
                        result += coefs[off++] * vars[i] * vars[j];
                    }
                }
                ++ringout[result % ring];
            }
            for (int sol_num : ringout) {
                ++out[sol_num];
            }
        }
        for (int i = 0; i < out.length; ++i) {
            System.out.println(i + " : " + out[i]);
        }
    }
}

Code 1. Degree 2, iterates over all polynomials.
## Table 1. Degree 2, rings 1 to 6.

| r:2 n:1 | r:3 n:1 | r:4 n:1 | r:5 n:1 | r:6 n:1 | r:6 n:4 |
|---------|---------|---------|---------|---------|---------|
| 0 2     | 0 8     | 0 26    | 0 44    | 0 102   | 0 237508496 |
| 1 4     | 1 12    | 1 16    | 1 40    | 1 48    | 36 15724800 |
| 2 2     | 2 6     | 2 20    | 2 40    | 2 48    | 54 50319360 |
| r:2 n:2 | 3 1     | 4 2     | 5 1     | 3 4     | 72 1292803200 |
| 0 4     |         |         |         |         | 4 12 84 3056901120 |
| 1 16    | 0 26    | 0 484   | 0 244   | 6 2     | 90 50319360 |
| 2 24    | 1 54    | 2 768   | 1 1000  | 342     | 7642252800  |
| 3 16    | 2 216   | 4 1872  | 4 6000  | 0 4476  | 108 1294088960 |
| 4 4     | 3 192   | 6 256   | 5 2640  | 1 864   | 120 6113802240 |
| r:2 n:3 | 4 108   | 8 696   | 6 4000  | 2 4752  | 126 9782083584 |
| 0 8     | 5 108   | 12 16   | 9 1500  | 3 3936  | 132 3821126400 |
| 2 224   | 6 24    | 16 4    | 10 240  | 4 7128  | 144 33045554880 |
| 4 560   | 9 1     |         |         |         | 5 1728  | 162 29121576960 |
| 6 224   |         |         |         |         | 6 8448  | 168 18996456960 |
| 8 8     | 0 80    | 8 218624| 0 1244  | 8 3456  | 180 2319888128 |
| r:2 n:4 | 3 702   | 12 114688| 5 31000 | 9 3088  | 192 4749114200 |
| 0 16    | 6 15444 | 16 364000| 20 3286000| 10 2592 | 198 12227604480 |
| 4 2240  | 9 27300 | 20 114688| 25 3175640| 12 3072 | 210 9782083584 |
| 6 7168  | 12 14040| 24 189952| 30 3224000| 15 1728 | 216 61472317440 |
| 8 13920 | 15 1404| 32 30128 | 45 46500 | 16 432  | 240 62448122880 |
| 10 7168 | 18 78   | 48 224  | 50 1240  | 18 408  | 252 3056901120 |
| 12 2240 | 27 1    | 64 8    | 125 1   | 20 432  | 264 23745571200 |
| 16 16   |         |         |         |         | 24 96   | 270 29222215680 |
| r:2 n:5 | 0 242   | 0 818704| 0 6244  | 27 16   | 288 14881950720 |
| 0 32    | 9 7020  | 16 114688| 25 806000| 36 4    | 300 1956167168 |
| 8 19840 | 18 533520| 32 707481600| 100 488436000 | r:6 n:3 | 324 9102215360 |
| 12 444416| 21 1364688| 40 44040192 | 105 2325000000 | 0 553672 | 330 12227604480 |
| 16 1168576| 24 3411720| 48 175472640 | 120 10075000000 | 6 157248 | 336 21835008 |
| 20 444416| 27 4062720| 56 44040192 | 125 3521540640 | 12 3852576 | 360 10032871680 |
| 24 19840| 30 2729376 | 64 401784000| 130 9300000000 | 18 6272448 | 384 54587520 |
| 32 32   | 33 1705860 | 72 73400320 | 145 2518750000 | 24 11799216 | 396 3821126400 |
| r:2 n:6 | 36 519480 | 80 119046144 | 150 486824000 | 30 314496 | 432 1231979520 |
| 0 64    | 45 14040 | 88 73400320 | 225 12090000 | 36 18764928 | 450 100638720 |
| 16 166656| 54 240   | 96 65020928 | 250 6240  | 48 7985952  | 480 43670016 |
| 24 18665472| 81 1    | 112 3440640 | 625 1  | 54 6115424 | 486 7168 |
| 28 56885248| r:3 n:5| 128 1373280 |         | 60 786240 | 528 27293760 |
| 32 117000576| 0 728 | 160 7168  |         | 72 3407040 | 540 33169920 |
| 36 56885248| 27 65340 | 192 2240 |         | 90 314496 | 576 8311680 |
| 40 18665472| 54 15550920| 256 16 |         | 96 1123200 | 648 551520 |
| 48 166656| 63 165127248 |         |         | 108 180320 | 720 224640 |
| 64 64   | 72 2642035968 |         |         | 120 112320 | 810 7168 |
| 81 4856139948 |         |         |         | 144 624 | 864 3840 |
| 90 2559472344 |         |         |         | 162 224 | 972 2240 |
| 99 206409060 |         |         |         | 216 8 | 1296 16 |

Table 1. Degree 2, rings 1 to 6.
Table 2. Degree 2, rings 7 to 12.
Table 3. Degree 2, rings 13 to 17.
| r:2 n:1 | r:3 n:3 | r:5 n:1 | r:6 n:1 | r:8 n:2 |
|---------|---------|---------|---------|---------|
| 0 4 0 52704 | 0 204 | 0 612 | 0 110516800 |
| 1 8 1 892296 | 1 260 | 1 288 | 4 304971776 |
| 2 4 2 5117580 | 2 120 | 2 288 | 8 332768256 |
| r:2 n:2 | r:5 n:2 | r:6 n:2 | r:8 n:2 | r:9 n:1 |
| 0 64 4 69599088 | 5 1 | 4 72 | 16 75890944 |
| 1 256 5 149433336 | 6 12 | 20 36962304 |
| 2 384 6 283362300 | 0 37204 | 24 10127360 |
| 3 256 7 442158912 | 3 40 | 283362300 |
| r:2 n:3 | r:4 n:2 | r:7 n:1 | r:8 n:2 | r:9 n:2 |
| 0 64 8 511758000 | 2 73200 | 1 1783296 | 32 1224576 |
| 1 4096 10 523357848 | 4 1682000 | 3 6041088 | 40 406080 |
| 2 32768 11 377165646 | 5 2043960 | 4 8574336 | 48 5376 |
| 2 114688 12 259619256 | 6 1520000 | 5 1741824 | 64 64 |
| 3 229376 13 156676680 | 7 1120000 | 6 10257408 |
| r:2 n:4 | r:4 n:3 | r:7 n:2 | r:8 n:2 | r:9 n:3 |
| 0 64 18 341172 | 13 8000 | 14 248832 | 6 18 |
| 1 1048576 21 25272 | 15 240 | 15 1741824 | 9 3 |
| 2 125829120 27 27 | 25 1 | 16 725760 | |
| r:3 n:1 | r:4 n:2 | r:7 n:1 | r:8 n:2 | r:9 n:2 |
| 0 24 16 64 | 1 631806 | 0 1764 | 24 19840464 |
| 1 36 | 2 3655008 | 1 1344 | 27 8782128 |
| 2 18 | 0 6982406144 | 3 15772512 | 2 592 | 33 1889568 |
| 3 3 | 4 45904560128 | 4 25486272 | 3 128 | 36 431244 |
| r:3 n:2 | r:4 n:3 | r:7 n:2 | r:8 n:2 | r:9 n:3 |
| 0 1530 | 12 236481150976 | 6 42065520 | 5 64 | 54 1512 |
| 1 6966 | 16 273363550208 | 7 46549440 | 6 16 | 63 64 |
| 2 13608 | 20 213360050176 | 8 37278612 | 12 3876804 | 8 4 |
| 3 16632 | 24 123153121280 | 9 34376832 |
| 4 11340 | 28 46368030720 | 10 19262880 |
| 5 6804 | 32 14964318208 | 11 12101040 |
| 6 1512 | 36 2392850432 | 12 5992896 |
| 7 648 | 40 551649280 | 13 3284568 |
| 9 9 | 44 14880064 | 14 595728 |
| r:4 n:1 | r:7 n:2 | r:8 n:2 | r:9 n:2 | r:10 n:1 |
| 0 100 | 56 32768 | 18 98784 |
| 1 80 | 64 4096 | 19 65856 |
| 2 56 | 21 1680 |
| 3 16 | 49 1 |
| 4 4 |

Table 4. Degree 3, rings 2 to 9.
Table 5. Degree 3, rings 10 to 14.

| r:10 | r:11 | r:12 | r:13 | r:14 |
|------|------|------|------|------|
| 0    | 4948 | 0    | 11844| 0    | 18305826496 |
| 1    | 2080 | 1    | 2880 | 1    | 12636 |
| 2    | 2000 | 2    | 3456 | 2    | 2808 |
| 3    | 320  | 3    | 816  | 3    | 3432 |
| 4    | 480  | 11   | 1152 | 13   | 4 |
| 5    | 8    |      | 6    | 456  |      |
| 6    | 160  |      | 8    | 72   | 17852028 |
| 7    | 4    |      |      | 9684 | 1 |
| 8    |      |      |      | 9684 | 1 |
| 9    |      |      |      | 9684 | 1 |
| 10   |      |      |      | 9684 | 1 |
| 11   | 598950 | 9  | 1634568 |
| 12   |      | 12  | 12   | 12   | 12 |
| 13   |      | 12  | 12   | 12   | 12 |
| 14   |      | 12  | 12   | 12   | 12 |

Table 5. Degree 3, rings 10 to 14.
| r:15 n:1 | r:15 n:2 (cont.) | r:16 n:1 | r:17 n:1 |
|----------|------------------|----------|----------|
| 0 26628  | 33 598752000    | 0 29668  | 0 28304  |
| 1 9360   | 35 8949466080   | 1 22528  | 1 37808  |
| 2 9000   | 36 6095904000   | 2 7488   | 2 6528   |
| 3 2220   | 39 1330560000   | 4 3152   | 3 10880  |
| 4 2160   | 40 5907568000   | 5 2048   | 17 1     |
| 5 36     | 42 2678400000   | 6 128    |          |
| 6 1080   | 44 4082400000   | 8 440    | 0 121251088 |
| 9 120    | 45 2203069320   | 10 64    | 1 8175232 |
| 10 18    | 48 9797760000   | 12 16    | 7 1086676992 |
| 15 3     | 49 7257600000   | 16 4     | 8 353170024 |

| r:15 n:2 | r:16 n:2 | r:17 n:2 |
|----------|----------|----------|
| 0 17081343126 | 52 907200000 | 0 115346070080 |
| 1 1455894000  | 54 498276000  | 8 315941191680 |
| 2 7943184000  | 55 2449440000 | 16 344032378880 |
| 3 12977172000 | 56 3810240000 | 24 195506995200 |
| 4 24047925000 | 60 2033942400 | 32 698525706240 |
| 5 15650261360 | 63 2177640000 | 40 347529543680 |
| 6 41640264000 | 65 5443200000 | 48 17423859712 |
| 7 7937352000  | 66 5443200000 | 56 41901069696 |
| 8 35285544000 | 70 6267456000 | 64 1390936320 |
| 9 24920532000 | 72 1738800000 | 72 611319808 |
| 10 33468872000| 75 1645952000 | 80 338952192 |
| 11 250776000  | 77 2323800000 | 88 85983232 |
| 12 65289456000| 78 1209600000 | 96 24020992 |
| 13 55728000   | 81 2884500000 | 104 9437184 |
| 14 15715296000| 84 5184000000 | 112 3211264 |
| 15 43277470560| 90 1233360000 | 128 1421184 |
| 16 27075884000| 91 5184000000 | 144 163840 |
| 18 31710960000| 99 3240000000 | 160 46080 |
| 19 39390000010| 100 11340000 | 192 5376 |
| 20 19511712000| 105 15552000 | 256 64 |
| 21 2489888000 | 108 7200000  | 34 36234168 |
| 22 29668464000| 117 7200000  | 35 1358346240 |
| 23 13907110800 | 125 6804 | 48 60370944 |
| 26 1088640000 | 135 2160   | 49 15092736 |
| 27 5342832000  | 150 1512   | 51 195840 |
| 28 13790736000 | 175 648   | 289 1 |
| 30 15044460480 | 225 9     |           |
| 32 66679200000 |          |           |

Table 6. Degree 3, rings 15 to 17.
In Tables 1 to 3 we present some outputs of such a program, whereas in Tables 4 to 6 we present outputs of an analogous program, yet with allowing the polynomials to have degree up to 3. Each section of those tables has a value \( r \) denoting size of the ring, and a value \( n \) which denotes number of variables. For example 3rd line in section for \( r : 3 \ n : 2 \) of table 1 says that there are 216 polynomials of degree up to 2, over the ring \( \mathbb{Z}_3 \) with 2 variables, that have precisely 2 solutions. In the tables we omitted those numbers of solutions for which there are no polynomials that have that many solutions. Additionally, to obtain those results we used a little more advanced programs, that iterated only once over many isomorphic polynomials, and, most importantly, were multi-threaded. We don’t present their code here, as it is long and doesn’t add much to this discussion. There are many interesting things that we can notice in the tables below. Because the number of solutions of any such polynomial has to be divisible by a certain constant, that number can occupy only one of the allowed “slots”. Yet, as we see, for a lot of those slots there are no polynomials that have that number of solutions. It also often happens, that several of the slots directly following the 0-slot are not taken. For example, in the section of Table 1 for \( r : 6 \ n : 4 \), the divisibility is 6, yet the smallest possible non-zero number of solutions is 36, which shows that this initial gap can be significantly larger than the divisibility. The earlier mentioned research by Clark, Forrow and Schmitt [14] is focused on counting the size of this first gap. It is important to mention that the gaps in the second half of the spectrum tend to be even larger. In the example we just looked at, half of the range is \( 1296/2 = 648 \), and there are only 5 slots “taken” after that half, whereas there are 39 taken slots up to that half. Additionally, the last gap, that is the difference between the two largest possible numbers of solutions, seems to be consistently the largest in all examples. This may be connected to the fact that also \( k \)-CNF has worse granularity on the number of satisfying assignments when the set of satisfying assignments is large. For example, a 3-CNF formula over \( n \) variables cannot have more than \( 7 \times 2^{n-3} \) satisfying assignments, unless it is a tautology. We directly present the sizes for the first and last gaps that we obtained in our experiments in Tables 15 to 17 that are close to the end of this chapter (columns go by the number of variables, and rows by the size of the ring). Another thing to notice is that, for example, each of the sections \( r : 2 \ n : 4 \), \( r : 4 \ n : 4 \), \( r : 6 \ n : 4 \) from Table 1 has certain numbers of solutions for which there are exactly 7168 and 2240 polynomials having that many solutions. There are also noticeable cases when number of polynomials having particular number of solutions is very small, when compared to neighbouring numbers. We can see this for example in Table 5 for \( r : 10 \ n : 4 \) for 25 solutions, and for \( r : 14 \ n : 4 \) in line for 49 solutions. We are sure that there are many other properties waiting to be noticed, and we contribute the above tables to facilitate future research and heuristic formulation in this area.

For phenomena we would like to especially focus our attention on, we provide Tables 7 to 10 for polynomials of degree up to 2, and Tables 11 to 14 for polynomials of degree up to 3. In all those tables the columns refer to number of variables of the polynomial, while the rows represent the size of the ring. For example, from Table 7 we can read that a polynomial of degree up to 2 over \( \mathbb{Z}_{12} \) with 4 variables must have its number of solutions be a multiple of 24; this follows by the theorem of [23]. Table 8 says for what percent of all polynomials their number of solutions is divisible by the minimum divisibility, and not by any higher power of the size of the ring. For example over \( \mathbb{Z}_2 \), half of the polynomials of 2 variables of degree up to 2 have the minimum divisibility of their solutions numbers (those are the polynomials that have 1 or 3 solutions in this case). Table 9 tells how many different numbers of solutions a polynomial over a given ring and number of variables may have. For example, polynomials over \( \mathbb{Z}_{11} \) with 2 variables (and still with degree up to 2), may only have one of 8 different solution numbers - in this case 0, 1, 10, 11, 12, 21, 22, and 121. Finally, the Table 10 gives the division, of the number of possible solutions numbers from Table 9 by the number of solutions numbers allowed by the minimum divisibility. For example over \( \mathbb{Z}_5 \) with 4 variables there is 12 possible solution numbers, whereas due to divisibility by 5, \( 125 + 1 = 126 \) slots are allowed. Then, \( 12/126 \) gives the 9.5% that we find in the table. Tables 11 to 14 are respectively analogous, but for polynomials of degree up to 3.

Having introduced the tables given below, let us discuss what we can learn from them. Tables 7 and 11 illustrate how much quicker the divisibility of solution numbers rises when we work over rings that include at least a second prime power, compared to when we work over fields. It is especially visible for the ring of size 16, in marked contrast to the ring \( \mathbb{Z}_{15} \) and the field \( \mathbb{Z}_{17} \). We see that the extension of the Ax’s theorem to non-field rings gives much greater divisibilities than the original Ax theorem does. This
divisibility gap grows even larger as we increase any of the following parameters: ring size, the number of variables, or the degree of the polynomial. It is also interesting to have a look at e.g. $\mathbb{Z}_{12}$, where we see that the divisibility of its solution numbers is a multiplication of divisibilities for $\mathbb{Z}_3$ and $\mathbb{Z}_4$ for the same $n$.

Tables 8 and 12 show us that a very large part of all the polynomials have the minimum divisibility allowed. This means, that if we would pick several polynomials at random, there is a high chance that at least one of them would have the minimum divisibility of its number of solutions. This is a very important observation; we based on it another program that we used, which will be shortly presented.

From Tables 9 and 13, we learn that the numbers of numbers of solutions the polynomials may have are surprisingly small. It would not be surprising at all, if those numbers of the “used slots” were bounded by a polynomial in the size of the ring $r$ and the number of variables $n$. For degree 2 it may even be a polynomial like $rn^k$, where $k$ is the number of prime divisors of $r$. Let us notice that for degree 2, for fields other than $\mathbb{Z}_2$, the numbers of used slots seem to be exactly the same, and they grow by 4 at every second increase in number of variables. Additionally, it seems that if for certain $\mathbb{Z}_x$ and $\mathbb{Z}_y$ the number of slots used don’t change between some numbers of variables $a$ and $b$, then also $\mathbb{Z}_{xy}$, has the same number of slots used for $n = a$ and $n = b$. For example for $\mathbb{Z}_2$, $\mathbb{Z}_5$, we consider $\mathbb{Z}_{10}$ with $n = 2$ and 3. This observation also strongly suggests that the number of slots used for $\mathbb{Z}_6$ and $n = 5$ is 44, even though we didn’t run an experiment which would confirm that.

The last pair of tables, 10 and 14, show that the fraction of slots allowed by minimum divisibility that are actually used, nearly always decreases with increasing number of variables. Even though the number of allowed slots increases exponentially, this strong decrease in how many of them are used gives hope that the ultimate number of used slots is actually only polynomially large. This has especially high probability of being true for fields and for rings over prime powers.

Other properties in this data seem to be worthy of further investigation. Many of them may be just mathematical curiosities, yet some may play a key role in understanding the shape of polynomial solutions spaces, and be fundamental in future results in low circuit complexity (especially $\text{ACC}^0[m]$), and also classical simulation of quantum circuits via polynomials.

The type of program that we used in the end to test our hypotheses is presented as the code 2. The user chooses ring size, vars num as the number of variables, div as the hypothetical divisibility of the number of solutions, and tries as the number of “tries” to check the hypothesis. The program counts numbers of solutions of tries-many randomly chosen polynomials of degree up to 3 over the given ring with the given number of variables. When the number of solutions of a checked polynomial is a multiple of div it passes silently, otherwise a remainder of the division of number of solutions by div is printed. The code is presented with ring=8, vars num=6, and div=512. The given divisibility is too large, as it should be only 256, therefore upon running this code we should see information of multiple remainders of 256, and the run won’t pass. We are highly likely to see polynomials that don’t have number of their solutions divisible by 512, even with the very small number of 50 tries. It is, because the fraction of polynomials that have minimum divisibility is very significant, as also tables 8 and 12 show. It may be true that when ring, degree and number of variables increase those fractions significantly decrease, yet even then most probably they still are not minuscule, and in our real experiments we were using large numbers of tries.
Table 7. Degree 2, minimum divisibility of number of solutions.

| r\n | 1 | 2 | 3 | 4 | 5 | 6 |
|-----|----|----|----|----|----|----|
| 2   | 1  | 1  | 2  | 2  | 4  | 4  |
| 3   | 1  | 1  | 3  | 3  | 9  | 9  |
| 4   | 1  | 2  | 4  | 8  | 16 | 32 |
| 5   | 1  | 1  | 5  | 5  | 25 | 25 |
| 6   | 1  | 1  | 6  | 6  | 36 | 36 |
| 7   | 1  | 1  | 7  | 7  | 49 | 49 |
| 8   | 1  | 4  | 16 | 32 | 128| 256|
| 9   | 1  | 3  | 9  | 27 | 81 | 243|
| 10  | 1  | 1  | 1  | 10 | 100| 100|
| 11  | 1  | 1  | 11 | 11 | 121| 121|
| 12  | 1  | 2  | 12 | 24 | 144| 288|
| 13  | 1  | 1  | 13 | 13 | 169| 169|
| 14  | 1  | 1  | 14 | 14 | 296| 296|
| 15  | 1  | 1  | 15 | 15 | 225| 225|
| 16  | 1  | 8  | 32 | 128| 512| 2048|
| 17  | 1  | 1  | 17 | 17 | 289| 289|

Table 8. Degree 2, percent of polynomials with number of solutions with minimum divisibility.

| r\n | 1 | 2 | 3 | 4 | 5 | 6 |
|-----|----|----|----|----|----|----|
| 2   | 50.0% | 50.0% | 43.8% | 43.8% | 42.4% | 42.4% |
| 3   | 66.7% | 66.7% | 53.5% | 64.2% | 53.3% |
| 4   | 25.0% | 25.0% | 21.9% | 21.9% |
| 5   | 64.0% | 80.0% | 67.5% | 79.4% |
| 6   | 51.9% | 64.6% | 62.4% | 62.9% |
| 7   | 61.2% | 85.7% | 75.3% |
| 8   | 25.0% | 37.5% | 19.1% |
| 9   | 44.6% | 59.3% | 21.4% |
| 10  | 48.4% | 83.5% | 81.2% |
| 11  | 57.9% | 90.9% | 83.4% |
| 12  | 40.5% | 62.4% | 47.6% |
| 13  | 56.8% | 92.3% | 85.8% |
| 14  | 46.1% | 86.6% | 85.5% |
| 15  | 45.6% | 84.2% | 84.0% |
| 16  | 25.0% | 31.3% | 5.5% |
| 17  | 55.4% | 94.1% | 88.9% |

Table 9. Degree 2, number of possible numbers of solutions.

| r\n | 1 | 2 | 3 | 4 | 5 | 6 |
|-----|----|----|----|----|----|----|
| 2   | 100.0% | 100.0% | 100.0% | 77.8% | 77.8% | 52.9% |
| 3   | 100.0% | 80.0% | 80.0% | 42.9% | 42.9% |
| 4   | 80.0% | 77.8% | 52.9% | 48.5% |
| 5   | 66.7% | 30.8% | 30.8% | 9.5% |
| 6   | 85.7% | 48.6% | 48.6% | 20.3% |
| 7   | 50.0% | 16.0% | 16.0% |
| 8   | 55.6% | 58.8% | 42.4% |
| 9   | 60.0% | 39.3% | 18.3% |
| 10  | 54.5% | 23.8% | 23.8% |
| 11  | 33.3% | 6.6% | 6.6% |
| 12  | 61.5% | 32.9% | 21.4% |
| 13  | 28.6% | 4.7% | 4.7% |
| 14  | 40.0% | 13.2% | 13.2% |
| 15  | 56.3% | 14.2% | 14.2% |
| 16  | 35.3% | 36.4% | 16.3% |
| 17  | 22.2% | 2.8% | 2.8% |

Table 10. Degree 2, percent of solution-number slots allowed by minimum divisibility, that are used.
| $r \ \backslash \ n$ | 1 | 2 | 3 | 4 | 5 | 6 |
|-----------------|---|---|---|---|---|---|
| 2               | 1 | 1 | 1 | 2 | 2 | 2 |
| 3               | 1 | 1 | 1 | 3 | 3 | 3 |
| 4               | 1 | 2 | 4 | 8 | 16 | 32 |
| 5               | 1 | 1 | 1 | 5 | 5 | 5 |
| 6               | 1 | 1 | 1 | 6 | 6 | 6 |
| 7               | 1 | 1 | 1 | 7 | 7 | 7 |
| 8               | 1 | 4 | 16 | 32 | 128 | 256 |
| 9               | 1 | 3 | 9 | 27 | 81 | 243 |
| 10              | 1 | 1 | 1 | 10 | 10 | 10 |
| 11              | 1 | 1 | 1 | 11 | 11 | 11 |
| 12              | 1 | 2 | 4 | 24 | 48 | 96 |
| 13              | 1 | 1 | 1 | 13 | 13 | 13 |
| 14              | 1 | 1 | 1 | 14 | 14 | 14 |
| 15              | 1 | 1 | 1 | 15 | 15 | 15 |
| 16              | 1 | 8 | 32 | 128 | 512 | 2048 |
| 17              | 1 | 1 | 1 | 17 | 17 | 17 |

Table 11. Degree 3, minimum divisibility of number of solutions.

| $r \ \backslash \ n$ | 1 | 2 | 3 | 4 |
|-----------------|---|---|---|---|
| 2               | 50.0% | 50.0% | 50% | 49.6% |
| 3               | 66.7% | 66.7% | 66.7% |
| 4               | 37.5% | 49.2% | 49.5% |
| 5               | 67.2% | 77.7% |
| 6               | 51.9% | 66.0% |
| 7               | 66.5% | 83.2% |
| 8               | 37.5% | 50.6% |
| 9               | 51.9% | 66.6% |
| 10              | 50.5% | 83.3% |
| 11              | 66.1% | 86.0% |
| 12              | 40.6% | 64.9% |
| 13              | 66.1% | 89.5% |
| 14              | 49.9% | 86.3% |
| 15              | 47.4% | 86.5% |
| 16              | 37.5% | 50.2% |
| 17              | 66.1% | 90.2% |

Table 12. Degree 3, percent of polynomials with number of solutions with minimum divisibility.

| $r \ \backslash \ n$ | 1 | 2 | 3 | 4 |
|-----------------|---|---|---|---|
| 2               | 100.0% | 100.0% | 100.0% | 100.0% |
| 3               | 100.0% | 90.0% | 78.6% |
| 4               | 100.0% | 88.9% | 88.2% |
| 5               | 83.3% | 61.5% |
| 6               | 85.7% | 59.5% |
| 7               | 62.5% | 40.0% |
| 8               | 88.9% | 76.5% |
| 9               | 70.0% | 57.1% |
| 10              | 72.7% | 39.6% |
| 11              | 41.7% | 22.1% |
| 12              | 69.2% | 45.2% |
| 13              | 35.7% | 17.1% |
| 14              | 53.3% | 25.4% |
| 15              | 62.5% | 29.2% |
| 16              | 58.8% | 60.6% |
| 17              | 27.8% | 10.7% |

Table 13. Degree 3, number of possible numbers of solutions.

Table 14. Degree 3, percent of solution-number slots allowed by minimum divisibility, that are used.
| r\n  | 1   | 2   | 3   | 4   | 5   | 6   |
|-----|-----|-----|-----|-----|-----|-----|
| 2   | 1   | 1   | 2   | 4   | 8   | 16  |
| 3   | 1   | 1   | 3   | 9   | 27  |
| 4   | 1   | 2   | 8   | 16  |
| 5   | 1   | 1   | 5   | 25  |
| 6   | 1   | 1   | 6   | 36  |
| 7   | 1   | 1   | 7   |
| 8   | 1   | 4   | 16  |
| 9   | 1   | 6   | 27  |
| 10  | 1   | 1   | 10  |
| 11  | 1   | 1   | 11  |
| 12  | 1   | 2   | 24  |
| 13  | 1   | 1   | 13  |
| 14  | 1   | 1   | 14  |
| 15  | 1   | 1   | 15  |
| 16  | 1   | 8   | 64  |
| 17  | 1   | 1   | 17  |

Table 15. Degree 2, size of the first gap between solution numbers.

| r\n  | 1   | 2   | 3   | 4   |
|-----|-----|-----|-----|-----|
| 2   | 1   | 1   | 2   | 4   |
| 3   | 1   | 1   | 2   | 6   |
| 4   | 1   | 2   | 4   |
| 5   | 1   | 1   | 2   | 10  |
| 6   | 1   | 1   | 2   | 8   |
| 7   | 1   | 1   | 2   | 28  |
| 8   | 1   | 4   | 2   | 16  |
| 9   | 1   | 3   | 3   | 18  |
| 10  | 1   | 1   | 4   | 25  |
| 11  | 1   | 1   | 8   | 88  |
| 12  | 1   | 2   | 3   | 32  |
| 13  | 1   | 1   | 10  | 130 |
| 14  | 1   | 1   | 7   | 49  |
| 15  | 1   | 1   | 5   | 50  |
| 16  | 1   | 8   | 4   | 64  |
| 17  | 1   | 1   | 14  | 17  |

Table 16. Degree 2, size of the last gap between solution numbers.

| r\n  | 1   | 2   | 3   | 4   |
|-----|-----|-----|-----|-----|
| 2   | 1   | 1   | 1   |
| 3   | 1   | 1   | 1   |
| 4   | 1   | 2   |
| 5   | 1   |
| 6   | 1   |
| 7   | 1   |
| 8   | 1   |
| 9   | 1   |
| 10  | 1   |
| 11  | 1   |
| 12  | 1   |
| 13  | 1   |
| 14  | 1   |
| 15  | 1   |
| 16  | 1   |
| 17  | 1   |

Table 17. Degree 3, size of the first gap between solution numbers.

| r\n  | 1   | 2   | 3   | 4   |
|-----|-----|-----|-----|-----|
| 2   | 1   | 1   | 1   |
| 3   | 1   | 1   |
| 4   | 1   |
| 5   | 1   |
| 6   | 1   |
| 7   | 1   |
| 8   | 1   |
| 9   | 1   |
| 10  | 1   |
| 11  | 1   |
| 12  | 1   |
| 13  | 1   |
| 14  | 1   |
| 15  | 1   |
| 16  | 1   |
| 17  | 1   |

Table 18. Degree 3, size of the last gap between solution numbers.
public class SolutionsRandom {

    public static boolean next(int[] arr, int ring) {
        for (int index = arr.length - 1; index >= 0; --index) {
            if (arr[index] < ring - 1) {
                arr[index] = ring - 1;
                return true;
            } else {
                arr[index] = 0;
            }
        }
        return false;
    }

    public static void main(String[] args) {
        int ring = 8;
        int vars_num = 6;
        int div = 512;
        int tries = 50;
        int coef_num = vars_num + (vars_num*(vars_num+1))/2 + (vars_num*(vars_num+1)*(vars_num+2))/6;
        int[] coefs = new int[coef_num];
        int[] vars = new int[vars_num];
        int[] ringout = new int[ring];
        for (int counter = 0; counter < tries; counter++) {
            for (int i = 0; i < coefs.length; i++) {
                coefs[i] = (int) (Math.random() * ring);
            }
            for (int i = 0; i < ring; ++i) {
                ringout[i] = 0;
            }
            for (int i = 0; i < vars_num; ++i) {
                vars[i] = 0;
            }
            vars[vars.length - 1] = -1;
            while (next(vars, ring)) {
                int result = 0;
                for (int i = 0; i < vars_num; ++i) {
                    result += coefs[i] * vars[i];
                }
                int off = vars_num;
                for (int i = 0; i < vars_num; ++i) {
                    for (int j = i; j < vars_num; ++j) {
                        result += coefs[off++] * vars[i] * vars[j];
                    }
                }
                for (int i = 0; i < vars_num; ++i) {
                    for (int j = i; j < vars_num; ++j) {
                        for (int k = j; k < vars_num; ++k) {
                            result += coefs[off++] * vars[i] * vars[j] * vars[k];
                        }
                    }
                }
                ++ringout[result % ring];
            }
            for (int sol_num : ringout) {
                int remainder = sol_num % div;
                if (remainder != 0) {
                    System.out.println("remainder: " + remainder);
                }
            }
        }
    }
}
6 Prospective applications in computer science

Polynomials modulo composite numbers represent the frontier of what is known in computational complexity theory, and a step beyond the well worked-out theory of polynomials over fields. In complexity theory they correspond to the class \( \text{ACC}^0 \) of languages represented by constant-depth, polynomial-sized circuits of Boolean and mod-\( m \) gates. That nonuniform \( \text{ACC} \) was only recently separated from the nondeterministic exponential time class \( \text{NEXP} \) [31] indicates how difficult they are to study. In mathematics there are strange behaviors even for univariate polynomials, for instance \( x \) “factors” as \((4x+3)(3x+4)\) over \( \mathbb{Z}_q \). Improving our understanding of their behavior may be of great use, when trying to prove more-strict lower bounds on \( \text{ACC}^0 \). It should be noted though, that the results are not directly translatable, as in circuits the inputs are limited only to \( \{0,1\} \), even when mod-\( m \) gates are being used. Moreover the bounds are unknown only when \( m \) has two or more prime factors. Still, greater knowledge of the solution-space structures for these \( m \) may help investigate the intersection with the image of the Boolean cube.

Cai, Chen, and Lu showed that counting number of solutions for polynomials of degree up to 2 in a ring of a fixed size is doable in polynomial time [7]. When the degree becomes 3 or higher, however, it is known to be \( \#\text{P–complete} \) in general [7]. The structure of solution spaces begun here, when further developed, may help map the boundary between feasible and hard cases in greater detail. This is especially important for the \( Z \)-function, where symmetry (or its lack) of solution cardinalities impacts the balance of the sum around the unit circle.

The application area that directly prompted this inquiry though, is the algebraic analysis of quantum circuits. Implicit or explicit in several well-known papers [2, 17, 15, 5] is the conversion of a quantum circuit \( C \) into a polynomial \( Q(\vec{y}) \) over \( \mathbb{Z}_m \) (where \( m \) is usually of the form \( 2^r \)) such that transition amplitude from input \( \vec{a} \) to output \( \vec{b} \) is given by

\[
\langle \vec{b} | U | \vec{a} \rangle = \frac{1}{R} \sum_{k=0}^{m-1} \#k_Q^* \cdot \omega^k
\]

where \( \omega = e^{2\pi i/m} \) and \( R \) is a normalizing constant depending only on \( C \). This form of the equivalent exponential sum \( \sum_{y} \omega^{Q(y)} \) emphasizes the role played by the solution-set cardinalities for the polynomials \( Q(\vec{y}) = k \) over all \( \vec{y} \). The one hitch (as above) is that \( \#k_Q^* \) restricts the count to those arguments \( \vec{y} = y_1 y_2 \cdots y_h \) that belong to the Boolean cube \( \{0,1\}^h \), taking it outside the immediate purview of the results for \( \#k_Q \) which range over all of \( \mathbb{Z}_m^h \).

However, in some cases there is a correspondence between \( \{0,1\}^h \) and \( \mathbb{Z}_m^h \) that enables carrying over the results. This is the case when \( C \) is a circuit of stabilizer gates, which produce a polynomial \( Q \) over \( \mathbb{Z}_4 \) consisting entirely of terms of the form \( y_i^2 \) or \( 2x_i y_j \) [26]. Then only the parities of \( y_i \) and \( y_j \) matter. The above-mentioned theorem of [7] then takes effect to show that the solution counts are polynomial-time computable, which yields yet-another-proof of the classical polynomial-time simulation of quantum stabilizer circuits [18] (see also [1]).

The divisibility of the numbers \( \#k_Q \) by large powers of the ring size, as proved by Marshall and Ramage [23], implies limitations on the range of values that this probability can take. In particular, it limits the ability to reduce the failure probability \( \epsilon \) of the measurement for a given size circuit—unless the circuit actually gives \( \epsilon = 0 \). The size is bounded below by the number \( h \) of nondeterministic gates (which generally are all Hadamard gates), which give rise to the variables \( \vec{y} = y_1, \ldots, y_h \).

7 Proof of Theorem 2

We present the proofs of the general induction step and the base case of Theorem 2 separately, respectively in subsections 7.a and 7.b.

7.a Proof of the general induction step

For any \( x \) in a ring \( \mathbb{Z}_{p^r} = \mathbb{Z}/p^r\mathbb{Z} \) where \( p \) is prime, let \( o(x) = \max \{ m : m \leq r \land p^m \mid x \} \) be the order of \( x \). The following lemma is a basic observation about the rings \( \mathbb{Z}_{2^r} \).
Lemma 1. Let \( h \in \mathbb{Z}_{2^r} \) and \( f = o(h) \). Then the following sets are equal as subsets of \( \mathbb{Z}_{2^r} \):

\[
\{ 2^f i : i \in \mathbb{Z}_{2^r} \} = \{ hi : i \in \mathbb{Z}_{2^r} \} = \{ hi : i \in \mathbb{Z}_{2^{r-1}} \}.
\]

Any such set described in the lemma above, contains all elements of the ring that share the same order. As an example, for \( \mathbb{Z}_{32} \), each such set contains all elements from a single level of the tree below, or it contains just the 0 element.

We will often use this lemma to change the order of iteration. For example,

\[
2^{q-1} - 1 \sum_{i=0}^{2^r-1} \{ 2^{r-q} i \} = 2^{q-1} - 1 \sum_{i=0}^{2^r-1} \{ (2k + 1)2^{r-q} i \} = 2^{q-1} - 1 \sum_{i=0}^{2^r-1} \{ (2^{r-q} + t2^{r-q+1}) i \}
\]

where \( q, t, k \) are any integers.

Theorem 2. (General induction step)

Let any quadratic polynomial \( Q \) of \( n \geq 4 \) variables \((x, z)\) over \( \mathbb{Z}_{2^r} \), and any integers \( q, v \leq r \) and \( k, w, g, u \), and any linear polynomial \( T(x) \) be given. Suppose that for any \( Q' \) of \( n - 1 \) variables \((x', z')\), any \( q', v' \leq r \) and \( k', w', g', u' \), and any linear polynomial \( T'(x') \) it holds that:

\[
\sum_{i=0}^{2^r-1} \sum_{j=0}^{2^{r'-1}-1} \#(k' + w'2^{r-q} j + g'2^{r-v} j)_{Q',z'=T'(x') + u'2^{r-v} j} = T'2^{\left\lceil \frac{n(n-2) + \min(2v, r)}{2} \right\rceil} + q' - 1
\]

for certain integer \( T' \). Then there is an integer \( T \) such that

\[
\sum_{i=0}^{2^{r-1}-1} \sum_{j=0}^{2^{r'-1}-1} \#(k + w2^{r-q} i + g2^{r-v} j)_{Q,z=T(x) + u2^{r-v} j} = T2^{\left\lceil \frac{n(n-1) + \min(2v, r)}{2} \right\rceil} + q - 1.
\]
Proof. Taking as the induction hypothesis that the theorem is true for all polynomials over \( n - 1 \) variables, we would like to show that it holds for any \( Q \) such that

\[
Q(x, z) = M(x, z) + mz^2,
\]

\[
M(x, z) = P(x) + L(x)z.
\]

Here \( Q \) and \( M \) are over \( n \) variables and have degree up to \( 2 \), \( P \) is over \( n - 1 \) variables and also has degree up to \( 2 \), \( L \) is a linear form over \( n - 1 \) variables and \( m \) is a constant. We will first prove the divisibility for \( M \) using the induction hypothesis for \( n - 1 \), and then we will prove divisibility of \( Q \), depending only on the result for \( M \).

Let us notice that

\[
\#kM,z=l = \sum_{h=0}^{2^r-1} \#(k-hl)_{P,L(x)=h}.
\]

We will frequently use decompositions of this form.

Let us move to proving the \( M \) part of the theorem, by which we mean the conclusion of Theorem 2 with \( M \) in place of \( Q \). We calculate:

\[
C = \sum_{i=0}^{2^s-1} \sum_{j=0}^{2^v-1} \#(k+w2^{r-q}i+g2^{r-v}j)_{M,z=1}(x)=T(x)+u2^{r-v}j = \sum_{i=0}^{2^s-1} \sum_{j=0}^{2^v-1} \#(k+w2^{r-q}i+g2^{r-v}j)_{U,z=2^{r-v}j},
\]

where \( U(x) = P(x) + L(x)(T(x) + uz) \). Let us write \( H(x) = P(x) + L(x)(T(x) + uz) - gz \) so that

\[
C = \sum_{i=0}^{2^s-1} \sum_{j=0}^{2^v-1} \#(k+w2^{r-q}i)_{H,z=2^{r-v}j}.
\]

Take \( w = o(w) \), that is write \( w = 2^mb \) where \( b \) is odd. By appeal to Lemma 1 we may ignore \( b \), so we have

\[
C = \sum_{i=0}^{2^s-1} \sum_{j=0}^{2^v-1} \#(k+2^{r-q+w}i)_{H,z=2^{r-v}j}.
\]

Now we can rewrite \( H = P'(x) + L'(x)z \) with certain \( P' \) no worse than quadratic, and importantly, certain linear \( L' \). Then we can further condition on all possible values \( h \) of \( L'(x) \), to obtain

\[
C = \sum_{i=0}^{2^s-1} \sum_{j=0}^{2^v-1} \sum_{h=0}^{2^s-1} \#(k+2^{r-q+w}i-2^{r-v}jh)_{H,L'(x)=h}.
\]

Considering all possible orders \( f \) of \( h \) separately then gives:

\[
C = \sum_{i=0}^{2^s-1} \sum_{j=0}^{2^v-1} \sum_{f=0}^{2^r-1} \sum_{h=0}^{2^s-1} \#(k+2^{r-q+w}i+2^{r-v}j2f(2h+1))_{H,L'(x)=2f(2h+1)}
\]

\[
+ \sum_{i=0}^{2^s-1} \sum_{j=0}^{2^v-1} \#(k+2^{r-q+w}i)_{H,L'(x)=0}.
\]

Let us divide the above sum into two parts \( C_1 \) and \( C_2 \) and consider them independently. The first part is for \( f \geq v \), and the second part is for the remaining orders \( f \leq v-1 \). Starting with the first part, we have:

\[
C_1 = \sum_{i=0}^{2^s-1} \sum_{j=0}^{2^v-1} \sum_{f=v}^{2^r-1} \sum_{h=0}^{2^s-1} \#(k+2^{r-q+w}i+2^{r-v}j(2h+1))_{H,L'(x)=2f(2h+1)}
\]

\[
+ \sum_{i=0}^{2^s-1} \sum_{j=0}^{2^v-1} \#(k+2^{r-q+w}i)_{H,L'(x)=0}.
\]
\[ \sum_{i=0}^{2^q-1} \sum_{j=0}^{2^r-1} \#(k + 2^{r-q+w} i)_{H,L'}(x) = 0 \]

Since \( f \geq v \), we get \( 2^r - v + f = 0 \), and therefore

\[ C_1 = 2^v \sum_{i=0}^{2^q-1} \sum_{h=0}^{2^r-1} \#(k + 2^{r-q+w} i)_{H,L'}(x) = 2^v h , \]

where we also collapsed orders of \( h \), by considering all of them when their order is at least \( v \) at once.

For certain values of \( h \), the condition \( L'(x) = 2^v h \) may be unsolvable. Let us take a variable \( y \) in \( x \) that is multiplied by some \( \alpha 2^\beta \) in \( L' \), such that \( \alpha \) is odd and no other variable in \( x \) is being multiplied in \( L' \) by a coefficient of a smaller order. Let \( \delta \) be the constant term in \( L' \). If the order of \( \delta \) is smaller than both \( \beta \) and \( v \), then \( L'(x) = 2^v h \) never has a solution and our whole expression becomes 0, which has any divisibility. When \( \alpha(\delta) \geq \min(\beta, v) \) then \( \delta \) only impacts which coset of set of solutions of \( L'(x) + \delta = 2^v h \) will be the solutions of \( L'(x) = 2^v h \). Therefore we can assume \( \delta = 0 \) without the loss of generality (\( h \) goes over the whole subring, while \( \alpha \) can be anything). Then \( L'(x) = 2^v h \) is solvable only when \( h = \gamma 2^{\max(\beta-v,0)} \) for certain \( \gamma \). For any such \( h \) we can solve the equation for \( y \) obtaining \( 2^\beta \) solutions of the form

\[ y_i = L'_{xy}(x-y) + \frac{\gamma 2^{\max(v-\beta,0)}}{\alpha} + i 2^{r-\beta}, \]

for \( i \) between 0 and \( 2^\beta - 1 \) and \( L'_{xy}(x-y) \) being over \( n - 2 \) variables and defined as: \( L'_{xy}(x-y) = (-L(x) + \alpha 2^\beta y)/\alpha 2^\beta \). Coming back to our sum \( C_1 \) as given earlier, we have:

\[ C_1 = 2^v \sum_{i=0}^{2^q-1} \sum_{h=0}^{2^r-1} \sum_{t=0}^{2^{r-\max(v,\beta)-1}} \#(k + 2^{r-q+w} i)_{H,L'}(x) = 2^v h \]

where we omitted \( h \)-s for which the constraint was always false. Carrying on,

\[ C_1 = 2^v \sum_{i=0}^{2^q-1} \sum_{h=0}^{2^r-\max(v,\beta)-1} \sum_{t=0}^{2^r-\max(v,\beta)-1} \#(k + 2^{r-q+w} i)_{H,L'}(x) = 2^v h + t 2^{r-\beta} \]

since \( \frac{2^{\max(v-\beta,0)}}{\alpha} h \) produces all values in \( \mathbb{Z}_{2^{r-\beta}} \) that are divisible by \( 2^{\max(v-\beta,0)} \), then \( t 2^{r-\beta} \) expands them to all such values in \( \mathbb{Z}_{2^{2r}} \). Hence

\[ C_1 = 2^v + \min(q,w) \sum_{i=0}^{2^{\max(q-w,0)-1}} \sum_{s=0}^{2^{\max(v,0)-1}} \sum_{t=0}^{2^{\max(v,0)-1}} \#(k + 2^{r-q+w} i)_{H,L'}(x) = 2^v + \min(q,w) T 2^{r(n-2) + \min(2r, 2^{\max(v,0)}, 2^\beta)} \]

which has possibly even more than the required divisibility. We used the induction hypothesis taking \( g \) to be 0 and \( T(x-y) = L_{xy}(x-y) \).
Let us look now at the second part, i.e. for \( f < v \):

\[
C_2 = \sum_{i=0}^{v-1} \sum_{j=0}^{2^v-1} \sum_{f=0}^{2^r-f-1-1} (k+2^{r-q}i+2^{r-v}f)_{H,L'(x)=2^f}\]

Again by appeal to Lemma 1,

\[
C_2 = \sum_{i=0}^{v-1} 2^{\min(q,w)+\min(v,f)} \sum_{j=0}^{2^\max(q-w,0)} \sum_{f=0}^{2^\max(v-f,0)} \sum_{h=0}^{2^r-f-1-1} (k+2^{r-q}i+2^{r-v}f)_{H,L'(x)=2^f+2^f+h}
\]

owing to the overlap of \( 2^{r-q}i \) and \( 2^{r-v}j \). Following steps are analogous to what we did in previous part: we solve \( L'(x) = 2^f + 2^f+h \) for a specific \( y \in x \) to obtain that \( C_2 \) equals the sum over \( f \) from 0 to \( v-1 \) of

\[2^{\min(q,w)+\min(v,f)+\max(\min(q-w,v-f),0)}\]

multiplied by

\[2^{\max(q-w,v-f)-1}2^{\max(f+1-\beta,0)-1}\]

This has the right form for applying the induction hypothesis, which gives us:

\[
C_2 = \sum_{f=0}^{v-1} 2^{\min(q,w)+\min(v,f)+\max(\min(q-w,v-f),0)} T^2 \left[ \frac{(r+n-2)\min(2r-2\max(f+1-\beta,0),r)}{2} + \max(q-w,v-f),0 \right] - 1
\]

\[
= \sum_{f=0}^{v-1} 2^{\min(q,w)+\min(v,f)+\max(\min(q,w),\min(v,f))} T^2 \left[ \frac{(r+n-2)\min(2r-2\max(f+1-\beta,0),r)}{2} + \max(q-w,v-f),0 \right] - 1
\]

\[
= \sum_{f=0}^{v-1} T^2 \left[ \frac{(r+n-1)\min(2r-2\max(f+1-\beta,0),r)}{2} + q + 1 \right] = \sum_{f=0}^{v-1} T^2 \left[ \frac{(r+n-1)\min(2r-2\max(f+1-\beta,0),r)}{2} + q - 1 \right]
\]

Thus \( C_2 \) has the required divisibility, since \( \max(f+1-v-\beta,-v) \leq 0 \) owing to \( f < v \). Hence so does \( C = C_1 + C_2 \). This proves the induction step for \( M \).

Having proved the divisibility property for \( M \), we may now use it in the proof for \( Q \):

\[
D = \sum_{i=0}^{2^v-1} \sum_{j=0}^{2^v-1} (k+2^{r-q}i+2^{r-v}j)_{Q,z=T(x)+u2^{r-v}j}
\]

\[
= \sum_{i=0}^{2^v-1} \sum_{j=0}^{2^v-1} (k+2^{r-q}i)_{G,z=2^{r-v}j},
\]

where \( G(x,z) = M(x) + T(x)L(x) + L(x)uz - gz + mT(x)^2 + 2muT(x)z + mu^2z^2 \) (we used analogous transformation as we did for \( M \) at the beginning of the proof). Let

\[
H(x,z) = M(x) + T(x)L(x) + L(x)uz - gz + mT(x)^2 + 2muT(x)z,
\]

23
which means $H$ has no square term for $z$, and its degree is up to 2. Later we will apply the divisibility we just proved for $M$, as induction hypothesis, to $H$. The sum we are working on equals

$$D = \sum_{i=0}^{2^k-1} \sum_{j=0}^{2^k-1} \#(k+w2^{r-q}i - mu^2(2^{r-v}j)^2)_{H,z=2^{r-v}j}$$

$$= \sum_{i=0}^{2^k-1} \sum_{j=0}^{2^k-1} \#(K(i)-t(2^{r-v}j)^2)_{H,z=2^{r-v}j},$$

where $K(i) = k + w2^{r-q}i$ and $t = mu^2$.

Now we iterate over $2^{r-v}j$, by going through all possible orders of it, as usual denoted by $f$. We have

$$D = \sum_{j=r-v}^{2^k-1} \sum_{i=0}^{2^k-1} \sum_{j=0}^{2^k-1-f-1} \#(K(i)-t(2^f(2j+1))^2)_{H,z=2^f(2j+1)} + \sum_{i=0}^{2^k-1} \#K(i)_{H,z=0}. \quad (1)$$

We consider cases when $r$ is even or odd separately. Let us first take $r$ to be even. From the sum 1 above, let us take any component of it having a single $f \leq \frac{r}{2} - 1$. We will show that each such a component has the required divisibility

$$\sum_{i=0}^{2^k-1} \sum_{j=0}^{2^k-1-f-1} \#(K(i)-t(2^f(2j+1))^2)_{H,z=2^f(2j+1)}$$

$$= \sum_{i=0}^{2^k-1} \sum_{j=0}^{2^k-1-f-1} \sum_{h=0}^{2^k-1} \#(K(i)-t((2j+1)(2^f+2^h))^2)_{H,z=(2j+1)(2^f+2^h)},$$

where we changed order of iteration on $z$ to consider it in groups that belong to subrings $\mathbb{Z}_{2r/z}$,

$$= \sum_{i=0}^{2^k-1} \sum_{j=0}^{2^k-1-f-1} \sum_{h=0}^{2^k-1} \#(K(i)-t((2j+1)(2^f+2^h))^2)_{H,z=(2j+1)(2^f+2^h)},$$

where we changed order of iteration for $h$ by multiplying by $2j+1$ which is odd (via Lemma 1),

$$= \sum_{j=0}^{2^k-f-1} \sum_{i=0}^{2^k-1} \sum_{h=0}^{2^k-1} \#(K(i)-t(2j+1)^2(2^f+2^h)^2)_{H,z=(2j+1)(2^f+2^h)}$$

$$= \sum_{j=0}^{2^k-f-1} \sum_{i=0}^{2^k-1} \sum_{h=0}^{2^k-1} \#(k-t(2j+1)^22^{2f}+w2^{r-q}i-t(2j+1)^22^{f+1}h)_{H,z=(2j+1)(2^f+2^h)}$$

$$= \sum_{j=0}^{2^k-f-1} \sum_{i=0}^{2^k-1} \sum_{h=0}^{2^k-1} T_j2^{\min(2^f, r)} + q-1 = \sum_{j=0}^{2^k-f-1} (T_j2^{\frac{r-n}{2}}[\frac{q}{2}])^{2^{f+1}} = \sum_{j=0}^{2^k-f-1} (T_j2^{\frac{r-n}{2}}),$$

which may even have a higher divisibility than required. We used the induction hypothesis with:

$$k' = k-t(2j+1)^22^{2f}$$

$$T'(x) = (2j+1)2^f$$

$$g' = -t(2j+1)^22^{f+1}$$

$$u' = (2j+1).$$
Let us note again, that we used the induction hypothesis for a polynomial of \(M\) with use of the induction hypothesis for \(f\).

Now we add and subtract 1 inside the expression

\[
\sum_{i=0}^{2^q-1} \sum_{j=0}^{2^q-\text{max}(\xi, r-v)-1} \#(K(i) - t(2^f(2j+1))^2)_{H,z=2^f(2j+1)} + \sum_{i=0}^{2^q-1} \#K(i)_{H,z=0}
\]

\[
= 2^q - 1^{r-1-1} \sum_{i=0}^{2^q-1} \sum_{j=0}^{2^q-\text{max}(\xi, r-v)-1} \#(K(i) - t(2^{\text{max}(\xi, r-v)}j)^2)_{H,z=2^{\text{max}(\xi, r-v)}j}
\]

\[
= 2^q - 1^{r-\text{max}(\xi, r-v)-1} \sum_{i=0}^{2^q-1} \sum_{j=0}^{2^q-\text{max}(\xi, r-v)-1} \#(k+w2^{r-q}i)_{H,z=2^{\text{max}(\xi, r-v)}j}
\]

\[
= \mathcal{T}2^q \frac{r(n-1) + \min(2(r-max(\xi, r-v)), r)}{2} + q - 1 = \mathcal{T}2^q \frac{r(n-1) + \min(2r, r)}{2} + q - 1,
\]

with use of the induction hypothesis for \(M\) of \(n\) variables.

Let us move now to the second case, that is when \(r\) is odd. First we take from \(D\), being written in

the form of the sum 1, any component for a single value of \(f\), such that \(f \leq \frac{r-1}{2} - 1\), and show that such a component has required divisibility:

\[
\sum_{i=0}^{2^q-1} \sum_{j=0}^{2^q-\text{max}(\xi, r-v)-1} \#(K(i) - t(2^f(2j+1))^2)_{H,z=2^f(2j+1)}
\]

\[
= 2^q - 1^{r-\frac{r-1}{2} - 1} \sum_{i=0}^{2^q-1} \sum_{j=0}^{2^q-\text{max}(\xi, r-v)-1} \#(K(i) - t(2^f(2j+1)+2^{\frac{r-1}{2}}h)^2)_{H,z=2^f(2j+1)+2^{\frac{r-1}{2}}h}
\]

\[
= \sum_{i=0}^{2^q-1} \sum_{j=0}^{2^q-\text{max}(\xi, r-v)-1} \sum_{h=0}^{2^q-\frac{r-1}{2}-1} \#(K(i) - t(2^f(2j+1)+2^{\frac{r-1}{2}}h)^2)_{H,z=(2j+1)(2f+2^{\frac{r-1}{2}}h)}
\]

Now we add and subtract 1 inside the expression:

\[
= \sum_{i=0}^{2^q-1} \sum_{j=0}^{2^q-\text{max}(\xi, r-v)-1} \sum_{h=0}^{2^q-\frac{r-1}{2}-1} \# \left( K(i) - t(2j+1)^2 \right)
\]

\[
\left( 2^{2f+2^{\frac{r-1}{2}}+h} + 2^{r-1}h^2 + 2^{\frac{r-1}{2}} \left( 2^{\frac{r-3}{2}} - 2^f \right) h - 2^{\frac{r-1}{2}} \left( 2^{\frac{r-3}{2}} - 2^f h \right) \right)_{H,z=(2j+1)(2f+2^{\frac{r-1}{2}}h)}
\]

\[
= \sum_{i=0}^{2^q-1} \sum_{j=0}^{2^q-\text{max}(\xi, r-v)-1} \sum_{h=0}^{2^q-\frac{r-1}{2}-1} \# \left( K(i) - t(2j+1)^2 \right)
\]

\[
\left( 2^{2f+2^{\frac{r-1}{2}}h} - 2^{r-1}h^2 + 2^{\frac{r-1}{2}} \left( 2^{\frac{r-3}{2}} - 2^f \right) h - 2^{\frac{r-1}{2}} \left( 2^{\frac{r-3}{2}} - 2^f h \right) \right)_{H,z=(2j+1)(2f+2^{\frac{r-1}{2}}h)}
\]

\[
= \sum_{i=0}^{2^q-1} \sum_{j=0}^{2^q-\text{max}(\xi, r-v)-1} \sum_{h=0}^{2^q-\frac{r-1}{2}-1} \# \left( K(i) - t(2j+1)^2 \right)
\]

\[
\left( 2^{2f+2^{\frac{r-1}{2}}h} h(2^f+2^{\frac{r-1}{2}}h)+2^{\frac{r-1}{2}} - 2^f \right) - 2^{\frac{r-1}{2}} \left( 2^{\frac{r-3}{2}} - 2^f h \right) \right)_{H,z=(2j+1)(2f+2^{\frac{r-1}{2}}h)}
\]
which may have even higher than required divisibility. The term $2^{r-1}h(h+1)$ always multiplies to $2^r$ so it cancels. We used the induction hypothesis of $M$ with:

$$k' = k-t(2j+1)^22^{2f}$$

$$T'(x) = (2j+1)2^f$$

$$g' = 2t(2j+1)^2(2^{r-3}-2^f)$$

$$u' = (2j+1).$$

Let us consider now those $f$-s from $D$ written as the sum 1 for which $f \geq \max(\frac{r-1}{2}, r-v)$:

$$D' = \sum_{f=\max(\frac{r-1}{2}, r-v)}^{r-1} \sum_{i=0}^{2^y-1} \sum_{j=0}^{2^{r-1}2^{r-1}-1} \#(K(i)-t(2f(2j+1))^2)_{H,z=2^y(2j+1)} + \sum_{i=0}^{2^y-1} \#K(i)_{H,z=0}$$

$$= \sum_{i=0}^{2^y-1} \sum_{j=0}^{2^{r-1}2^{\max(\frac{r-1}{2}, r-v)-1}} \#(K(i)-t(2^{\max(\frac{r-1}{2}, r-v)})^2)_{H,z=2^{\max(\frac{r-1}{2}, r-v)}}$$

$$= \sum_{i=0}^{2^y-1} \sum_{j=0}^{2^{r-1}2^{\max(\frac{r-1}{2}, r-v)-1}} \#(K(i)-t2^{\max(r-1, 2(r-v))})_{H,z=2^{\max(\frac{r-1}{2}, r-v)}}.$$
Below we will work with multisets. We will use a “multiplicative” notation to represent them. For example,

\[2\{1\} = \{1,1\}; \quad 3\{1,3\} \cup 2\{2\} = \{1,1,1,2,2,3,3,3\}; \quad 2 \bigcup_{i=0}^{1} \{3i\} = \{0,0,3,3\}.

**Lemma 3.** Let us take a polynomial \(P(x) = ax^2 + bx + c\) over \(\mathbb{Z}_{2^r}\). Let \(a = q2^w\) and \(b = q2^h\) such that \(q\) and \(g\) are odd and \(w, h\) are orders of respectively \(a\) and \(b\). Let \(m = \min(w, h)\). The image of \(P(x)\) treated as a multiset equals

a) If \(w > h\):

\[2^m \bigcup_{i=0}^{2^r-m-1} \{2^m i + c\}\]

b) If \(w = h\):

\[2^m + 1 \bigcup_{i=0}^{2^r-m-1} \left\{2^m i + c\right\} \quad \text{if } m < r
\]

\[2^r \{c\} \quad \text{if } m = r
\]

c) If \(w < h\):

\[
\left(\left\lceil \frac{m}{w} \right\rceil - 1 \sum_{j=0}^{r-2m-1} 2^{min(f+2r-f-1)+\min(m,\max(0,r-2f-3)) \bigcup_{i=0}^{\max(0,2^r-2f-3-m-1)} \{2^{2f+3+m} i + q2^{2f+m} + t\}}\right) \\
\quad \cup 2\left\lceil \frac{m}{w} \right\rceil \{t\}
\]

where \(t = c - \frac{q}{2^w + q}\). □

Let us introduce now a concept of a slice, which is a coset of an ideal of a ring. If we look at the multiset that the image of \(P\) in above corollary is, then in cases a) and b) it is just a single slice (possibly with each distinct element having multiple occurrences). In the case c) the image of \(P\) is built from multiple slices, one for each \(f\) between 0 and \(\left\lfloor \frac{r-m}{w} \right\rfloor - 1\), and then a final slice \(\{t\}\).

Let us say we would be interested in an intersection between the images of two functions \(P(x)\) and \(Q(y)\). More precisely we would want to evaluate:

\[\#\{(x, y) : P(x) = Q(y)\}.
\]

To start with, for sake of intuition, let’s suppose we are working over \(\mathbb{Z}_3\) (i.e., both functions have a 3-element domain), and that the image of \(P\) is \(\{0, 1, 1\}\) (with \(P(0) = 0\)) while the image of \(Q\) is \(\{1, 1, 1\}\). Then

\[\{(x, y) : P(x) = Q(y)\} = \{(1, 0), (1, 1), (1, 2), (2, 0), (2, 1), (2, 2)\}
\]

and the size of the intersection of the images is 6. When we look directly at the multisets \(\{0, 1, 1\}\) and \(\{1, 1, 1\}\) that the images constitute, we would like the intersection of them, as we understand it, to be also of size 6. This gives rise to the “multiplicative” intersection concept, which in our example is

\[\{(1, 1), (1, 1), (1, 1), (1, 1), (1, 1), (1, 1)\}.
\]

That is, each element from the first image is paired up with each element of the second image that it is equal to. For another example, the intersection of \(\{1, 1, 2\}\) and \(\{1, 2, 3\}\) is deemed to be

\[\{(1, 1), (1, 1), (2, 2)\}.
\]
In general, if the first multiset has distinct elements \( p_i \) with respective numbers of occurrences \( a_i \), and the second multiset has distinct elements \( q_j \) with numbers of occurrences \( b_j \), then the size of their intersection is deemed to be
\[
\sum_{i,j:p_i=q_j} a_i b_j.
\]
As synonyms of “intersection” we will also say “common elements” or “overlap.”

**Corollary 2.** Let \( P(x) = a_x x^2 + b_x x + c_x \) and \( Q(y, h) = a_y y^2 + b_y y + c_y + 2^{-d} h \) where \( d \leq r \). Then for any \( v, q \in [d, r] \), when we work over \( \mathbb{Z}_{2^r} \) it holds that:
\[
2^{\min(v,q)+d} \# \left\{ (x, y, h) : x \in \bigcup_{j=0}^{2^r-1} \{ l_x + 2^{-v} j \}, y \in \bigcup_{j=0}^{2^q-1} \{ l_y + 2^{-q} j \}, h \in \bigcup_{j=0}^{2^d-1} \{ j \}, P(x) = Q(y, h) \right\}
\]
for any \( l_x, l_y \), where \( | \cdot | \) stands for divides.

When proving the base induction step of our main theorem we will come against a specific multiset that a polynomial we will have may potentially intersect with. The following corollary gives us the divisibility of the size of such an intersection.

**Corollary 3.** Let us work over a ring \( \mathbb{Z}_{2^r} \). Let \( P(x) = a_x x^2 + b_x x + c \) with \( x \) being constrained to domain \( x \in \bigcup_{j=0}^{2^r-1} \{ l_x + 2^{-v} j \} \) for certain \( l_x \) and \( v \leq r \). Let \( S \) be the following multiset
\[
\left( \bigcup_{i=0}^{2^r-1} f_s \bigcup_{s=0}^{2^r-v-1} \{ 2^{r-v} i + 2^{r-v} i + f_s (2s + 1) \} \right) \cup \left( \bigcup_{i=0}^{2^r-1} (v+1) \{ 2^{r-v} i \} \right)
\]
where \( e \leq \min(q, v) \). The number of elements of the intersection (understood as the “multiplicative” intersection) of the multiset \( S \) and the image of \( P \) is divisible by
\[
2^{e+\min(q,v,\left\lfloor \frac{r}{2} \right\rfloor)}.
\]

**Theorem 2.** (Base case)
For any polynomial \( Q \) of \( 3 \) variables \( (x, y, z) \) over \( \mathbb{Z}_{2^r} \) of degree up to \( 2 \), any integers \( q, v \leq r \) and \( k, w, g, u \) and any linear polynomial \( T(x, y) \), it holds that:
\[
\sum_{i=0}^{2^r-1} \sum_{j=0}^{2^r-1} \#(k+w 2^{-q} i + g 2^{r-v} j) Q_{z=T(x,y)+u 2^{-v} j} = T 2^{r+\left\lfloor \frac{\min(2^q,r)}{2} \right\rfloor + q-1}
\]
for certain integer \( T \).

**Proof.** Note that when proving \( M \) part in the general induction step we use as induction hypothesis polynomials over \( n-1 \) variables, whereas when proving \( Q \) part we use polynomials on \( n \) variables, just without a square term in \( z \). Therefore for the base step we just need to prove that
\[
\sum_{i=0}^{2^r-1} \sum_{j=0}^{2^r-1} \#(k+w 2^{-q} i + g 2^{r-v} j) M_{z=T(x,y)+u 2^{-v} j} = T 2^{r+\min(v,\left\lfloor \frac{r}{2} \right\rfloor) + q-1},
\]
where
\[
M(x, y, z) = P(x, y) + L_z(x, y) z,
\]
\( L \) is a linear form, and \( P \) has degree up to \( 2 \). The transition from \( M \) to \( Q \) for \( n = 3 \) is already taken care of by the general induction step. Here we begin:
\[
\sum_{i=0}^{2^r-1} \sum_{j=0}^{2^r-1} \#(k+w 2^{-q} i + g 2^{r-v} j) M_{z=T(x,y)+u 2^{r-v} j} = \sum_{i=0}^{2^r-1} \sum_{j=0}^{2^r-1} \#(k+w 2^{-q} i + g 2^{r-v} j) U_{z=u 2^{r-v} j}
\]
28
where \( U(x, y, z) = P(x, y) + T(x, y)L_z(x, y) + L_z(x, y)z \)
\[
= \sum_{i=0}^{2^v-1} \sum_{j=0}^{2^v-1} \#(k+2^r-q\cdot w)_{R, z=2^r-v}\]

where \( R(x, y, z) = P(x, y) + T(x, y)L_z(x, y) + L'_z(x, y)z, L'_z(x, y) = uL_z(x, y) - g \) and \( w \) is the order of \( \omega \),
\[
= 2^{\min(q, w)} \sum_{i=0}^{2^\max(q-w, 0)-1} \sum_{j=0}^{2^v-1} \#(k+2^r-q\cdot w)_{R, z=2^r-v}\]
\[
= 2^{\min(q, w)} \sum_{i=0}^{2^v-1} \sum_{j=0}^{2^v-1} \#(k+2^r-w)_{R, z=2^r-v}\]

where \( e = \max(q - w, 0) \). Let us ignore the \( 2^{\min(q, w)} \) coefficient, and focus on the sum:
\[
W = \sum_{i=0}^{2^v-1} \sum_{j=0}^{2^v-1} \#(k+2^r-w)_{R, z=2^r-v}\]

for which we need to show that it is divisible by \( 2^{r+\min(v, \lceil \frac{r}{2} \rceil)}+e-1 \). We have
\[
W = \sum_{i=0}^{2^v-1} \sum_{j=0}^{2^v-1} \sum_{l=0}^{2^r} \#(k+2^r-w)_{G, L'_z(x, y) = l}\]

where \( G(x, y) = P(x, y) + T(x, y)L_z(x, y) \). Let \( L'_z(x, y) = \alpha_2 2^y + \zeta_2 2^v x + \delta_z \), where \( \alpha_z \) and \( \zeta_z \) are odd and we assume without the loss of generality that \( \beta_z \leq \eta_z \). Then,
\[
W = \sum_{i=0}^{2^v-1} \sum_{j=0}^{2^v-1} \sum_{l=0}^{2^r} \#(k+2^r-w)_{G, L'_z(x, y) = 2^\beta_z l + \delta_z}\]

as always \( 2^{\beta_z} | L'_z(x, y) - \delta_z \),
\[
= \sum_{i=0}^{2^v-1} \sum_{j=0}^{2^v-1} \sum_{l=0}^{2^r} \sum_{s=0}^{2^r} \#(k+2^r-w)_{G, y = \frac{1}{\alpha_z} + \frac{s}{\alpha_z} 2^\beta_z x + 2^r s}\]

where we solved \( L'_z(x, y) = 2^\beta_z l + \delta_z \) for \( y \). Taking \( G(x, y) = E(x) + L_y(x)y + my^2 \), for certain up to quadratic \( E \) and linear \( L_y \) we can write:
\[
W = \sum_{i=0}^{2^v-1} \sum_{j=0}^{2^v-1} \sum_{l=0}^{2^r} \sum_{s=0}^{2^r} \#(k+2^r-w)_{L'_y(x, y) + 2^r s}\]

where \( U(x, y) = E(x) + L_y(x)(\frac{1}{\alpha_z} 2^n - \beta_z x + y) + m(\frac{1}{\alpha_z} 2^n - \beta_z x)^2 + 2m \frac{1}{\alpha_z} 2^n - \beta_z xy + my^2 = E'(x) + L'_y(x)y + my^2 \) for certain up to quadratic \( E' \) and linear \( L'_y \).
\[
W = \sum_{i=0}^{2^v-1} \sum_{j=0}^{2^v-1} \sum_{l=0}^{2^v-1} \sum_{s=0}^{2^r} \#(k+2^r-w)_{U, y = s}\]

where \( O(s) = \alpha_z 2^\beta_z (s \mod 2^r) + \delta_z = \alpha_z 2^\beta_z s + \delta_z \),
\[
= \sum_{i=0}^{2^v-1} \sum_{j=0}^{2^v-1} \sum_{l=0}^{2^r} \sum_{s=0}^{2^r} \#(k+2^r-w)_{O(s) 2^r j - hs - ms^2}\]

where \( \alpha_z 2^\beta_z (s \mod 2^r) + \delta_z \).
\[ W = \sum_{i=0}^{2^v-1} \sum_{j=0}^{2^e-1} \sum_{s=0}^{2^{r-v}+\beta z} \sum_{h=0}^{2^{v+\gamma z}+1} \#(k+2^{r-v}i - 2^{r-v}j - (\alpha z 2^{r-v}+\beta z j + h)s - m s^2) E', L'_w(x)=h \]
as \( \min(\gamma_z, v) + \min(e, \max(v - \gamma_z, 0)) \) + \( d = e + v \), recall that \( d = \max(e, v - \gamma_z) \).

Now we can use Corollary 2. Solving \( L'_y(x) = 2^{h(1+2h)} \) for \( x \) will give us a certain slice in which \( x \) has to be, and the size of that slice will be at least \( 2^{r-f_h-1} \). Therefore the expression

\[
2^{\max(r-f_h-s_f,d)-1} 2^{r-f_h-1-1} \sum_{s=0}^l \sum_{h=0} \#(k-2^{\min(f_h+g_f,r-d)}) E', L'_y(x) = 2^{h(1+2h)}
\]

equals the size of the common part of image of \( E'(x) \) with \( x \) in the just mentioned slice, and image of function \( k+2^{\min(f_h+g_f,r-d)} \) (with \( s \) in a slice of size \( 2^{\max(r-f_h-g_f,d)} \)). Due to Corollary 2, this expression is divisible by \( 2^{r-f_h-1} \) (size of smaller domain, \( d = 0 \) in the corollary use). Therefore, and because \( r - d \geq 1 \), we have

\[
S_1 = 2^{r+v} \sum_{f_h=0}^l 2^{\min(r-d,f_h+g_f)} T_{f_h} 2^{r-f_h-1} = 2^{r+v+v-1} \sum_{f_h=0}^l 2^{u_f} T_{f_h},
\]

where \( u_f = 0 \) or 1. This gives possibly even more than the desired divisibility.

When moving to the part of \( S \), written as the sum (3), where \( r - v + \beta_z > f_h > \min(r - d, m) \), let us consider two cases, either \( r - d \leq m \) or \( r - d > m \). Let us start with the first of them, and let us consider it now together with the second sum from \( W \) written in the form (2)

\[
K = 2^{\min(\gamma_z,v)+\min(e,\max(v-\gamma_z,0))} \sum_{i=0}^{2^d-1} \sum_{s=0}^{2^d-1} \sum_{f_h=r-d+1}^{2^{r-f_h-1}-1} \sum_{h=0} \#(k+2^{r-i} f - s - ms^2) E', L'_y(x) = 2^{h(1+2h)}
\]

\[
+ \sum_{i=0}^{2^d-1} \sum_{j=0}^{2^d-1} \sum_{s=0}^{2^d-1} \sum_{h=0} \#(k+2^{r-i} i - 2^{r-v+\gamma_z} j - (\alpha'_z 2^{r-v+\beta_z} j + 2^{r-v+\beta_z} h)s - ms^2) E', L'_y(x) = 2^{r+v+\beta_z h}
\]

noting that both of \( f^h s \) and \(-\alpha'_z 2^{r-v+\beta_z} j + 2^{r-v+\beta_z} h)s - ms^2 \) have smaller “granularity” than \( 2^{r-d} j \) (the latter, because we assumed for this case that \( m \geq r - d \) and indirectly that \( \beta_z > \gamma_z \)). Continuing,

\[
K = 2^{r+\min(\gamma_z,v)+\min(e,\max(v-\gamma_z,0))} \sum_{i=0}^{2^d-1} \sum_{s=0}^{2^d-1} \sum_{h=0} \#(k+2^{r-i} f - s - ms^2) E', L'_y(x) = 2^{r-v+\beta_z h},
\]

(in this case we have an assumption that \( d \geq 1 \), due to \( f_h > r-d \))

\[
= 2^{r+\min(\gamma_z,v)+\min(e,\max(v-\gamma_z,0))} \sum_{i=0}^{\frac{2^d-1}{2}} \sum_{h=0} \#(k+2^{r-i} f - s - ms^2) E', L'_y(x) = 2^{r-v+\beta_z h},
\]

which gives the desired divisibility. We once again used Corollary 2, in the same way as for the previous case.

Let us now move to the case when \( r - d > m \):

\[
K = 2^{\min(\gamma_z,v)+\min(e,\max(v-\gamma_z,0))} \sum_{i=0}^{2^d-1} \sum_{s=0}^{2^d-1} \sum_{f_h=m+1}^{2^{r-f_h-1}-1} \sum_{h=0} \#(k+2^{r-i} f - s - ms^2) E', L'_y(x) = 2^{h(1+2h)}
\]

\[
+ \sum_{i=0}^{2^d-1} \sum_{j=0}^{2^d-1} \sum_{s=0}^{2^d-1} \sum_{h=0} \#(k+2^{r-i} i - 2^{r-v+\gamma_z} j - (\alpha'_z 2^{r-v+\beta_z} j + 2^{r-v+\beta_z} h)s - ms^2) E', L'_y(x) = 2^{r-v+\beta_z h}
\]
\[
\begin{align*}
&= 2^{\min(\gamma_z,v) + \min(e,\max(v-\gamma_z,0))} \sum_{i=0}^{2^d-1} \sum_{j=0}^{2^d-1-2^{-v+\beta_z-1}} \sum_{s=0}^{2^d-1-2^{-v+\beta_z-1}} \sum_{h=0}^{f_h=m+1} \sum_{h=0}^{2^{r-d}} #(k+2^{r-d}i - ms^2)_{E',L'_h(x)=2^h(1+2h)} \\
&+ 2^{\min(\gamma_z,v) + \min(e,\max(v-\gamma_z,0))} \sum_{i=0}^{2^d-1} \sum_{j=0}^{2^d-1} \sum_{s=0}^{2^d-1} \sum_{h=0}^{2^{r-d}} #(k+2^{r-d}i - ms^2)_{E',L'_h(x)=2^{r-v+\beta_z}h} \\
\end{align*}
\]

(since both polynomials on \(s\) are of type \(e\), per Lemma 3)

\[
\begin{align*}
&= 2^{\min(\gamma_z,v) + \min(e,\max(v-\gamma_z,0))} \sum_{i=0}^{2^d-1} \sum_{j=0}^{2^d-1-2^{-m-1-1}} \sum_{s=0}^{2^d-1} \sum_{h=0}^{2^{r-d}} #(k+2^{r-d}i - 2^m s^2)_{E',L'_h(x)=2^{m+1}h} \\
&= 2^{\min(\gamma_z,v) + \min(e,\max(v-\gamma_z,0))} \sum_{i=0}^{2^d-1} \sum_{j=0}^{2^d-1-2^{-m-1-1}} \sum_{s=0}^{2^d-1} \sum_{h=0}^{2^{r-d}} #(k+2^{r-d}i - 2^m s^2)_{E',L'_h(x)=2^{m+1}h} \\
&= 2^{\min(\gamma_z,v) + \min(e,\max(v-\gamma_z,0)) + m} \sum_{i=0}^{2^d-1} \sum_{j=0}^{2^d-1-2^{-m-1}} \sum_{s=0}^{2^d-1} \sum_{h=0}^{2^{r-d}} #(k+2^{r-d}i - 2^m s^2)_{E',L'_h(x)=2^{m+1}h} \\
&= 2^{\min(\gamma_z,v) + \min(e,\max(v-\gamma_z,0)) + m} \mathcal{T} 2^{r-m-1+d}, \\
\end{align*}
\]

where we used Corollary 2 remembering that \(r - d > m \Leftrightarrow r - m - 1 \geq d\). So finally

\[
K = 2^{r+v+u+1} \mathcal{T}
\]

which in this case gives possibly even more than the required divisibility.

Now we are left with the situation when \(\min(r-d,m) \geq r - v + \beta_z\), and we already know that \(S\), i.e. the first sum from \(W\) written in the form \((2)\), has the desired divisibility. Let us look now at the second of the two sums of \(W\):

\[
C = \sum_{i=0}^{2^d-1} \sum_{j=0}^{2^d-1} \sum_{s=0}^{2^d-1} \sum_{h=0}^{2^d-1} \sum_{s=0}^{2^d-1} \sum_{h=0}^{2^d-1} \sum_{h=0}^{2^{r-d}} #(k+2^r-i - 2^{v-v+\gamma_z}j - (\alpha_z' 2^{r-v+\beta_z} j + 2^{r-v+\beta_z} h) s - m s^2)_{E',L'_h(x)=2^{r-v+\beta_z}h} \\
\]

Because \(r - v + \gamma_z \geq r - v + \beta_z\), we can let \(\sigma_z = \gamma_z - \beta_z\), where \(\sigma_z \geq 0\). Then we have:

\[
C = \sum_{i=0}^{2^d-1} \sum_{j=0}^{2^d-1} \sum_{s=0}^{2^d-1} \sum_{h=0}^{2^d-1} \sum_{h=0}^{2^{r-d}} #(k+2^r-i - 2^{r-v+\beta_z} (\alpha_z'' 2^{\sigma_z} j + (j + h) s - m s^2)_{E',L'_h(x)=2^{r-v+\beta_z}h}, \\
\]

where \(\alpha_z'' = \alpha_z'^{-1}\). Because

\[
\alpha_z'' 2^{\sigma_z} j + (j + h) s = (j + h)(\alpha_z'' 2^{\sigma_z} s) + \alpha_z'' 2^{\sigma_z} h, \\
\]

we obtain

\[
C = \sum_{i=0}^{2^d-1} \sum_{j=0}^{2^d-1} \sum_{s=0}^{2^d-1} \sum_{h=0}^{2^d-1} \sum_{h=0}^{2^{r-d}} #(k+2^r-i - 2^{r-v+\beta_z} (j + h)(\alpha_z'' 2^{\sigma_z} s) - m s^2 - \alpha_z'' 2^{r-v+\gamma_z} h)_{E',L'_h(x)=2^{r-v+\beta_z}h}, \\
\]

We are operating now under an assumption that \(r - v + \beta_z \leq m\), therefore \(C\) equals

\[
2^{r-v} \sum_{i=0}^{2^d-1} \sum_{j=0}^{2^d-1} \sum_{s=0}^{2^d-1} \sum_{h=0}^{2^d-1} \sum_{h=0}^{2^{r-d}} #(k+2^r-i - 2^{r-v+\beta_z} ((j + h)(\alpha_z'' 2^{\sigma_z} s) - m 2^{m'} s^2) - \alpha_z'' 2^{r-v+\gamma_z} h)_{E',L'_h(x)=2^{r-v+\beta_z}h}, \\
\]

where \(m' = m - (r - v + \beta_z)\), and \(m\) is the odd factor in \(m\). Let us notice now that:

\[
\bigcup_{j,s \in \mathbb{Z}_{2^d}} \left\{(j + h)(\alpha_z'' 2^{\sigma_z} s) - m 2^{m'} s^2\right\} = \bigcup_{j,s \in \mathbb{Z}_{2^d}} \left\{\alpha_z'' 2^{\sigma_z} (j + h) + s(j + h - m 2^{m'} s)\right\} \\
\]

32
where we changed the starting point of the iteration on \( j \) by \( m2^m \),
\[
\bigcup_{s,j \in \mathbb{Z}_{2^m}} \{ \alpha'^{\nu+2\sigma_z}(j + h + m2^m s) + s(j + h) \}
\]
where we changed the starting point of the iteration on \( j \) by an additional \( m2^m \),
\[
\bigcup_{s,j \in \mathbb{Z}_{2^m}} \{ \alpha'^{\nu+2\sigma_z}(j + h + m2^m \alpha'^{\nu+2\sigma_z}) + s(j + h) \}
\]
where we changed the starting point of the iteration on \( j \) by an additional \( h \),
\[
\bigcup_{s,j \in \mathbb{Z}_{2^m}} \{-ma_z^2\alpha'^{\nu+2\sigma_z} + j(s + \alpha'^{\nu+2\sigma_z}) \} = \bigcup_{s,j \in \mathbb{Z}_{2^m}} \{ -ma_z^2\alpha'^{\nu+2\sigma_z} + js \}.
\]
The last follows because \( \bigcup_{s \in \mathbb{Z}_{2^m}} \{ s + \alpha'^{\nu+2\sigma_z} \} = \bigcup_{s \in \mathbb{Z}_{2^m}} \{ s \} \). Going back to our original formula we can write that:
\[
C = 2^{r+v-2^v-1} \sum_{i=0}^{2^v-1} \sum_{j=0}^{r-v} \sum_{s=0}^{2^v-1} \sum_{h=0}^{2^v-1} \sum_{\beta_z=0}^{2^v-1} \text{#}(k + 2^{r-v}i - 2^{r-v}j - 2^{r-v} \beta_z (j + \alpha'^{\nu+2\sigma_z} h) E', L'_s(x) = 2^{r-v} \beta_z h)
\]
\[
= 2^{r-v-2^v+2^{\min(v, \beta_z)}} \sum_{i=0}^{2^v-1} \sum_{j=0}^{2^v-1} \sum_{s=0}^{2^v-1} \sum_{h=0}^{2^v-1} \sum_{\beta_z=0}^{2^v-1} \text{#}(k' + 2^{v+2\beta_z}i - 2^{r-v} j - 2^{r-v} \beta_z (j + \alpha'^{\nu+2\sigma_z} h) E', L'_s(x) = 2^{r-v} \beta_z h)
\]
where \( v' = v - \beta_z \). If \( v' \leq 0 \), then \( e = 0 \), since \( \min(r - d, m) \geq r + \beta_z \) in this case, and \( d = \max(e, v - \gamma_z) \). In such a case \( C \) becomes
\[
2^{r+v} \#k'_{E', L'_s(x) = 0},
\]
which trivially divides by \( 2^{r+e+\min(v, [\frac{v}{2}])} \). Let us continue our proof now with the assumption that \( v' > 0 \), for which our formula is
\[
C = 2^{r-v+2\beta_z} \sum_{i=0}^{2^{v'-1} - 2^{v'-1}} \sum_{j=0}^{2^{v'-1} - 2^{v'-1}} \sum_{s=0}^{2^{v'-1} - 2^{v'-1}} \sum_{h=0}^{2^{v'-1} - 2^{v'-1}} \text{#}(k' + 2^{v'-1}i - 2^{r-v'} j - 2^{r-v'} (s + \alpha'^{\nu+2\sigma_z} h) E', L'_s(x) = 2^{r-v'} h)
\]
We use Lemma 2 on \( js, \) and \( j \) and \( s \) are now confined to the ring \( \mathbb{Z}_{2^{v'}} \):
\[
C = 2^{r-v+2\beta_z} \sum_{i=0}^{2^{v'-1} - 2^{v'-1}} \sum_{j=0}^{2^{v'-1} - 2^{v'-1}} \sum_{s=0}^{2^{v'-1} - 2^{v'-1}} (O(s) + 1)2^{v'-1} \text{#}(k' + 2^{v'-1}i - 2^{r-v'} (s + \alpha'^{\nu+2\sigma_z} h) E', L'_s(x) = 2^{r-v'} h),
\]

33
(where $O(s)$ is the order of $s$, unless $s = 0$, when it is the order (i.e. $v'$) increased by 1)

$$
2^{r+\beta_x-1} \sum_{i=0}^{2^{r'-1} - 2^{r'-1} - 1} \sum_{s=0}^{2^{r'-1} - 2^{r'-1} - 1} \sum_{h=0}^{2^{r'-1} - 1} (O(s) + 1)(k' + 2^{r'-e}i - 2^{r'-v'}(s - \alpha_2^{v'}2^{r}h))_{E',L'_y(x)=2^{r-v'}h}
$$

$$
= 2^{r+\beta_x-1} \sum_{i=0}^{2^{r'-1} - 2^{r'-1} - 1} \sum_{s=0}^{2^{r'-1} - 2^{r'-1} - 1} \sum_{h=0}^{2^{r'-1} - 1} (O(s) + 1)(k' + 2^{r'-e}i - 2^{r'-v'}s)_{E',L'_y(x)=2^{r-v'}h}.
$$

The last follows because for any $h$,

$$
\bigcup_{s=0}^{2^{v'-1} - 1} 2^{r-v'}s = \bigcup_{s=0}^{2^{v'-1} - 1} 2^{r-v'}(s - \alpha_2^{v'}2^{r}h).
$$

To increase clarity, let us omit the $2^{r+\beta_x-1}$ coefficient. We need to show that

$$
2^{e + \min(v', \lceil \frac{e}{2} \rceil)}
$$

divides the remaining sum

$$
C_1 = \sum_{i=0}^{2^{r'-1} - 2^{r'-1} - 1} \sum_{s=0}^{2^{r'-1} - 2^{r'-1} - 1} \sum_{h=0}^{2^{r'-1} - 1} (O(s) + 1)(k' + 2^{r'-e}i - 2^{r'-v'}s)_{E',L'_y(x)=2^{r-v'}h},
$$

or even just

$$
C_2 = \sum_{i=0}^{2^{r'-1} - 2^{r'-1} - 1} \sum_{s=0}^{2^{r'-1} - 2^{r'-1} - 1} \sum_{h=0}^{2^{r'-1} - 1} O(s)(k' + 2^{r'-e}i - 2^{r'-v'}s)_{E',L'_y(x)=2^{r-v'}h},
$$

since it is easy to show using our earlier techniques that

$$
\sum_{i=0}^{2^{r'-1} - 2^{r'-1} - 1} \sum_{s=0}^{2^{r'-1} - 2^{r'-1} - 1} \sum_{h=0}^{2^{r'-1} - 1} #(k' + 2^{r'-e}i - 2^{r'-v'}s)_{E',L'_y(x)=2^{r-v'}h}
$$

is divisible by $2^{r+v'}$ (via Corollary 2).

Focusing on $C_2$, let us split it into the possible orders $f_s$ of $s$:

$$
\begin{align*}
C_2 &= \sum_{i=0}^{2^{r'-1} - 2^{r'-1} - 1} \sum_{s=0}^{2^{v'-1} - 1} \sum_{h=0}^{2^{r'-1} - 1} O(s)(k' + 2^{r'-e}i - 2^{r'-v'}s)_{E',L'_y(x)=2^{r-v'}h} \\
&= \left( \sum_{h=0}^{2^{v'-1} - 1} \sum_{i=0}^{2^{r'-1} - 1} \sum_{s=0}^{2^{v'-1} - 1} f_s \sum_{s=0}^{2^{v'-1} - 1} #(k' + 2^{r'-e}i - 2^{r'-v'}(2s + 1))_{E',L'_y(x)=2^{r-v'}h} \right) \\
&\quad + \left( \sum_{h=0}^{2^{v'-1} - 1} \sum_{i=0}^{2^{r'-1} - 1} (v' + 1)#(k' + 2^{r'-v'}i)_{E',L'_y(x)=2^{r-v'}h} \right).
\end{align*}
$$

Solving $L'_y(x) = 2^{r-v'}h$ for $x$ with $h \in \mathbb{Z}_{2^{v'}}$ confines $x$ to a certain slice of size at least $2^{v'}$, which then becomes the domain of $E'$. Therefore the expression

$$
\sum_{i=0}^{2^{r'-1} - 1} \sum_{s=0}^{2^{r'-1} - 1} f_s \sum_{s=0}^{2^{r'-1} - 1} #(k' + 2^{r'-e}i - 2^{r'-v'}(2s + 1))_{E',L'_y(x)=2^{r-v'}h}
$$

34
equals the size of the common part of the image of $E'(x)$ with $x$ in the just mentioned slice, and the multiset
\[
\bigcup_{i=0}^{2^r-1} \bigcup_{s=0}^{2^r-1} \bigcup_{f_i=0}^{2^r-f_i-1-1} \{k' + 2r - e_i - 2r - e'(2s + 1)\}.
\]
This works analogously to the second component of the sum above, and allows us to directly use Corollary 3, recalling that $e \leq e'$ as $r - e \geq r - v + \beta v$ in this case. The polynomial $E'$ corresponds to $P$, and the multiset we obtain here from both components of the sum corresponds to the multiset $S$ (we just need to shift both of them by $k'$). By use of the corollary we obtain that our formula is divisible by
\[
2^{r + \min(v', \lceil \frac{v}{2} \rceil)},
\]
which at last concludes the proof of the base case and the entire theorem from the stated lemmas. 

We remark that the most difficult juncture of the above proof seems to be the treatment of multipliciti- es in the intersections. Even in better-behaved cases of algebraic varieties defined by polynomials over fields, intersection theory is known as a relatively difficult subject. It is possible that carrying over some of this theory to $\mathbb{Z}_{2^r}$ may improve the conceptual highness of abstraction in the proof, but we have not seen how to do this.

The rest of this chapter—amounting to most of it—gives proofs of the lemmas and corollaries stated earlier in this section, as well as some new ones that are needed for their proofs. This requires more situational analysis of intersections and multiplicities.

**Lemma 2. (restated)** For any $m \in \mathbb{Z}_{2^r}$,
\[
\# \{x, y \in \mathbb{Z}_{2^r} : xy = m\} = \begin{cases} (o(m) + 1)2^{r-1} & \text{if } m \neq 0, \\ (r + 2)2^{r-1} & \text{otherwise.} \end{cases}
\]

**Proof.** Let us start with the case $m \neq 0$. Let us notice that
\[
\forall t < r, \# \{m \in \mathbb{Z}_{2^r} : o(m) = t\} = 2^{r-t-1} \quad \text{and} \quad xy = m \Rightarrow o(x) + o(y) = o(m).
\]
To find the number of pairs $x, y$ such that $o(x) + o(y) = o(m)$, we can start by first taking pairs where $o(x) = 0$ and $o(y) = o(m)$, and go all the way until $o(x) = o(m)$ and $o(y) = 0$. It gives us:
\[
\forall t < r, \sum_{m \in \mathbb{Z}_{2^r}, o(m) = t} \# \{x, y \in \mathbb{Z}_{2^r} : xy = m\} = \sum_{i=0}^{t} 2^{r-1-i}2^{r-t-1+i}
\]
Because of symmetry,
\[
\# \{x, y \in \mathbb{Z}_{2^r} : xy = m\} = \frac{\sum_{m' \in \mathbb{Z}_{2^r}, o(m') = o(m)} \# \{x, y \in \mathbb{Z}_{2^r} : xy = m'\}}{\# \{m' \in \mathbb{Z}_{2^r} : o(m') = o(m)\}}.
\]
Therefore, with $t = o(m)$:
\[
\# \{x, y \in \mathbb{Z}_{2^r} : xy = m\} = \sum_{i=0}^{t} 2^{r-2-t} = (t + 1)2^{r-1}.
\]
For $m = 0$, let us just subtract from all pairs, those pairs for cases when $m > 0$:
\[
\# \{x, y \in \mathbb{Z}_{2^r} : xy = 0\} = 2^{2r} - \sum_{t=0}^{r-1} \sum_{i=0}^{t} 2^{2r-2-t},
\]
which after some transformations (including use of the formula for the sum of arithmetic-geometric series) gives the desired result. 

\[35\]
Lemma 4. For any \( t \in \mathbb{Z}_2^r \) there is a \( k \in \mathbb{Z}_2^r \) such that

\[
t^2 = 2^{2a(t)} + 2^{2a(t) + 3}k.
\]

Additionally following holds:

\[
\forall a, k \in \mathbb{Z}_2^r : t^2 = 2^{2a} + 2^{2a+3}k,
\]

where:

\[
n = \begin{cases} 
2 \min(a+2r, a-1) & \text{if } a < \frac{r}{2} \\
2^\lfloor \frac{a}{2} \rfloor & \text{otherwise}
\end{cases}
\]

Moreover, when \( a < \frac{r}{2} \) then the order of all such \( t \)-s equals \( a \).

Proof. Let \( q \) be the order of \( t \). Then \( t = 2^q(1 + 2m) \) for some \( m \), and \( t^2 = 2^{2q} + 2^{2q+2}m(m+1) = 2^{2q} + 2^{2q+3}k \) for certain \( k \). This proves the first part of the lemma.

Now let us show that

\[
\forall a < \frac{r}{2}, t \in \mathbb{Z}_2^r : t^2 \equiv 2^{2a} + 2^{2a+3}k \pmod{2^r}.
\]

We choose \( t = 2^q(1 + 2m) \), and obtain:

\[
(2^q(1 + 2m))^2 \equiv 2^{2q} + 2^{2q+3}k \pmod{2^r},
\]

\[
1 + 4m + 4m^2 \equiv 1 + 8k \pmod{2^r-2^a}.
\]

If \( r - 2a < 3 \) the above is true for any \( m \) and \( k \). Otherwise:

\[
m^2 + m \equiv 2k \pmod{2^{r-2a-2}}.
\]

We show that the last statement from above is true (i.e. for any \( k \) there is an \( m \) making it true) through induction on \( r \) and the use of Hensel lifting. Let us take \( P(m) = m^2 + m - 2k \), and let us note that \( \forall m. P'(m) \neq 0 \) modulo any non-zero power of \( 2 \) \( (P' \) being the derivative of \( P \)). This allows us to use Hensel’s lemma, which in this case says that if

\[
m^2 + m - 2k \equiv 0 \pmod{2^{r-1}}
\]

has a solution, then also

\[
m^2 + m - 2k \equiv 0 \pmod{2^r}
\]

does. Checking the base case of \( r = 1 \) is trivial. Therefore we have that \( \forall a < \frac{r}{2}, t \in \mathbb{Z}_2^r : t^2 = 2^{2a} + 2^{2a+3}k \), and that \( o(t) = a \). Let us take \( a < \frac{r}{2} - 1 \), then:

\[
t^2 \equiv (2^{r-a-1} + t)^2 \equiv (2 \cdot 2^{r-a-1} + t)^2 \equiv \ldots \equiv ((2^{a+1} - 1) \cdot 2^{r-a-1} + t)^2
\]

\[
\equiv (2^{r-a-1} - t)^2 \equiv (2 \cdot 2^{r-a-1} - t)^2 \equiv \ldots \equiv (2^{a+1} \cdot 2^{r-a-1} - t)^2 \pmod{2^r}.
\]

The numbers in those squares are all different (to wit, \( t \) and \( 2^{r-a-1} - t \) are different, all because \( a < \frac{r}{2} - 1 \). There are exactly \( 2a+2 \) of those numbers. Those are also all such numbers whose squares equal \( 2^{2a} + 2^{2a+3}k \). It is because for a given \( a \) there are \( 2^{r-a-1} \) numbers with order \( a \), and there are also \( 2^{r-2a-3} \) possible values to which squares of them can evaluate. If we find for any such square value \( 2^{a+2} \)-many \( t \)-s that evaluate to it, then we obtain \( 2^{r-2a-3+a+2} = 2^{r-a-1} \), which means we have found all such \( t \)-s.

The remaining options for \( a < \frac{r}{2} \) are when \( a = \frac{r+1}{2} \) (i.e. \( r \) is odd) or \( a = \frac{r}{2} - 1 \) (i.e. \( r \) is even). For \( a = \frac{r+1}{2} \) we have

\[
t^2 \equiv (2^{r-a} + t)^2 \equiv (2 \cdot 2^{r-a} + t)^2 \equiv \ldots \equiv ((2^a - 1) \cdot 2^{r-a} + t)^2,
\]

and there are exactly \( 2^a = 2^{r-a-1} \) of those numbers. Meanwhile for \( a = \frac{r}{2} - 1 \) we obtain

\[
t^2 \equiv (2^{r-a-1} + t)^2 \equiv (2 \cdot 2^{r-a-1} + t)^2 \equiv \ldots \equiv ((2^{a+1} - 1) \cdot 2^{r-a-1} + t)^2 \pmod{2^r},
\]

36
and there are exactly $2^{a+1} = 2^{r-a-1}$ of those numbers. In the last two cases, it is straightforward to see, that we have found all applicable numbers $t$, after all there are exactly $2^{r-a-1}$ numbers of order $a$.

Combining the above results, we can write that when $a < \frac{r}{2}$, we get $2^\min(a+2,r-a-1)$ of the numbers $t$ that we look for.

Now let us look at the case when $a \geq \frac{r}{2}$. Then any square of a number of order $a$ has to evaluate to $0$. And there are $2^r - \lceil \frac{r}{2} \rceil = 2^\lfloor \frac{r}{2} \rfloor$ numbers that have such orders. No number of any lower order can have its square evaluate to $0$.

**Lemma 3. (restated)**

Let us take a polynomial $P(x) = ax^2 + bx + c$ over $\mathbb{Z}_2$. Let $a = q^{2w}$ and $b = g^{2h}$ such that $q$ and $g$ are odd and $w, h$ are orders of respectively $a$ and $b$. Let $m = \min(w, h)$. The image of $P(x)$ treated as a multiset equals:

a) If $w > h$:

$$2^m \bigcup_{i=0}^{2^{r-m}-1} \{2^m i + c\}$$

b) If $w = h$:

$$2^{m+1} \bigcup_{i=0}^{2^{r-m}-1} \{2^{m+1} i + c\} \quad \text{if } m < r$$

$$2^r \{c\} \quad \text{if } m = r$$

c) If $w < h$:

$$\left(\bigcup_{f=0}^{\lceil \frac{r}{2} \rceil} \bigcup_{i=0}^{\max(0, 2^{r-2f-3-m-1})} \{2^{2f+3+m} i + q^{2^f+m} + t\}\right)$$

$$\bigcup 2^\lfloor \frac{r}{2} \rfloor \{t\}$$

where $t = c - \frac{q^2}{2^{2m-w}}$.

**Proof.** We prove each of the cases on its own:

a) $w > h$:

First we show that:

$$\forall i \in \mathbb{Z}_2, \exists x \in \mathbb{Z}_2 : q^{2w-m}x^2 + gx \equiv i \pmod{2^r}$$

We do this by induction on $r$ with the use of Hensel’s lemma. The base step for $r = 1$ is easy to check. For the general step, let us take $Q(x) = q^{2w-m}x^2 + gx - i$ and notice that regardless of $x$, $Q'(x)$ is always odd. This means, via Hensel’s lemma, that if $t$ is a solution of $Q(x)$ over $2^r$, then there is also a unique solution $S(t)$ that solves $Q(x)$ over $2^{r+1}$, and $S$ is a bijection. Due to the above we obtain that

$$\bigcup_{x=0}^{2^{r-1}} \{q^{2w-m}x^2 + gx\} = \bigcup_{i=0}^{2^{r-1}} \{i\},$$

which after multiplying both sides by $2^m$ and adding $c$ gives us the expected result.

b) $w = h$:

Analogous to the above, by the use of Hensel’s lemma we obtain that:

$$\forall i \in \mathbb{Z}_2, \exists x \in \mathbb{Z}_2 : qx^2 + gx \equiv 2i \pmod{2^r},$$

37
Let us start by removing $c$:

\[ qx^2 + g^{2h-m}x = q\left( x^2 + \frac{g}{q}g^{2h-m}x \right) = q\left( x + \frac{g}{q}g^{2h-m-1} \right)^2 - \left( \frac{g}{q}g^{2h-m-1} \right)^2, \]

which after multiplying both sides by $2^m$ and adding $c$ gives us the desired result.

c) $w < h$:

Let us start by removing $c$ from $P$ and dividing it by $2^m$ (we will introduce these factors back later):

\[ qx^2 + g^{2h-m}x = q\left( x^2 + \frac{g}{q}g^{2h-m}x \right) = q\left( x + \frac{g}{q}g^{2h-m-1} \right)^2 \]

and by use of Lemma 4,

\[ = \left( \left[ \frac{q}{g}g^{2h-m-1} \right]^{-1} \bigcup_{f=0}^{\min(f+2,r-f-1)} 2^{\max(0,2r-2f-3)-1} \bigcup_{i=0}^{\max(0,2r-2f-3)} \{2^{2f+3}i + 2^{2f} \} \right) \cup 2\left[ \frac{q}{g} \right] \{0\}. \]

After shifting the elements by $\left( \frac{g}{q}g^{2h-m-1} \right)^2 = \left( \frac{b}{2m+1}q \right)^2$ and multiplying them by $q$, this gives:

\[ = \left( \left[ \frac{q}{g}g^{2h-m-1} \right]^{-1} \bigcup_{f=0}^{\min(f+2,r-f-1)} 2^{\max(0,2r-2f-3)-1} \bigcup_{i=0}^{\max(0,2r-2f-3)} \{q\left( 2^{2f+3}i + 2^{2f} - \left( \frac{b}{2m+1}q \right)^2 \right) \} \right) \]

\[ \cup 2\left[ \frac{q}{g} \right] \left\{ -q \left( \frac{b}{2m+1}q \right)^2 \right\}, \]

which after multiplying the elements by $2^m$ and then shifting by $c$ is:

\[ = \left( \left[ \frac{q}{g}g^{2h-m-1} \right]^{-1} \bigcup_{f=0}^{\min(f+2,r-f-1)+\min(m,\max(0,r-2f-3))} 2^{\max(0,2r-2f-3-m)-1} \bigcup_{i=0}^{\max(0,2r-2f-3-m)} \{2^{2f+3}i + q2^{2f+m} \} \right) \]

\[ \cup 2\left[ \frac{q}{g} \right] \{t\} \]

\[ = \left( \left[ \frac{q}{g}g^{2h-m-1} \right]^{-1} \bigcup_{f=0}^{\min(f+2,r-f-1)+\min(m,\max(0,r-2f-3))} 2^{\max(0,2r-2f-3-m)-1} \bigcup_{i=0}^{\max(0,2r-2f-3-m)} \{2^{2f+3}i + q2^{2f+m} \} \right) \]

\[ \cup 2\left[ \frac{q}{g} \right] \{t\}. \]

We could remove $q$ that was multiplied by $2^{2f+3+m}i$ owing to Lemma 1.
Corollary 4. Let us take a polynomial \( P(x) = ax^2 + bx + c \), over \( \mathbb{Z}_{2^r} \) with the domain restricted to \( \bigcup_{j=0}^{2^r-1} \{l + 2^{r-v}j\} \) where \( v \leq r, l \in \mathbb{Z}_{2^r} \). Let \( k = r - v \), \( a' = a2^{2k} \), \( b' = (2al + b)2^k \), \( c' = al^2 + bl + c \). Let \( a' = q'2^{w'} \) and \( b' = g'2^{h'} \) such that \( q' \) and \( g' \) are odd and \( w', h' \) are orders of respectively \( a' \) and \( b' \). Let \( m' = \min(w', h', r) \). The co-domain of \( P(x) \) treated as a multiset equals:

\[ a) \text{ If } w' > h': \]
\[ 2^{m'-k} \sum_{i=0}^{2^{r-m'-1}} \{2^{m'i + c'}\} \]

\[ b) \text{ If } w' = h': \]
\[ 2^{m'+1-k} \sum_{i=0}^{2^{r-m'-1}} \{2^{m'+1i + c'}\} \quad \text{if } m' < r \\
2^{r-k}\{c'\} \quad \text{if } m' = r \]

\[ c) \text{ If } w' < h': \]
\[ \left( \sum_{f=0}^{\left\lfloor \frac{m'}{2} \right\rfloor} 2^{\min(f+2r-f-1)+\min(m', \max(0, r-2f-3))} \right)^{\max(0, 2^{r-2f-3-m'})} \]
\[ \sum_{i=0}^{2^{r-m'-1}} \{2^{2f+3+m' i + q'2f+m' + t'}\} \]
\[ \cup 2 \left\lfloor \frac{r+m'}{2} \right\rfloor - k \{t'\} \]

where \( t' = c' - \frac{b'2q}{2^{m'+2q}} \)

Proof. Any \( x \) in the domain can be written as \( l + 2^k j \) for certain \( j \), and therefore:
\[ ax^2 + bx + c = a(l + 2^r j)^2 + b(l + 2^r j) + c = a2^{2k}j^2 + (a2^{k+1}l + b2^k)j + al^2 + bl + c, \]

from which the mapping to variables with primes automatically follows. Finally, we need to divide the number of occurrences of each element of the multiset by \( 2^k \), as we have just \( 2^r = 2^{r-k} \)-many \( j \)'s.

In the following lemma we take a slice for a single \( f \) from category \( c) \), and count how many elements it has.

Lemma 5. Let us define a multiset \( S \) over \( \mathbb{Z}_{2^r} \) by
\[ S = 2^{\min(f+2r-f-1)+\min(m', \max(0, r-2f-3))} \sum_{i=0}^{2^{r-2f-3-m'-1}} \{2^{2f+3+m' i + q'2f+m' + t'}\}, \]

where all constants are integers between \( 0 \) and \( r \) inclusive, \( f \leq \left\lfloor \frac{r-m'}{2} \right\rfloor - 1 \), and \( r > m' \geq k \). The number of elements of the multiset \( S \) equals
\[ 2^{r-f-k-1}. \]

Proof. The number of elements of \( S \) is
\[ \#S = 2^{\max(0, r-2f-3-m')} \min(f+2r-f-1)+\min(m', \max(0, r-2f-3))}, \]
Let us go through following cases:

\[ \bullet \ 0 > r - 2f - 3: \]
\[ \#S = 2^{q+r-f-1+0-k} = 2^{r-f-k-1} \]
• \( r - 2f - 3 \geq 0 > r - 2f - 3 - m' \):
\[
\#S = 2^{f+2+\min(m', r-2f-3)-k} = 2^{f+2+r-2f-3-k} = 2^{r-f-k-1}
\]
• \( r - 2f - 3 - m' \geq 0 \):
\[
\#S = 2^{r-2f-3-m'+f+2+m'-k} = 2^{r-f-k-1}.
\]

In the next lemma we count the number of elements of slices for a single \( f \), all \( f' > f \), and also the slice \( \{t'\} \).

**Lemma 6.** Let us define a multiset \( S \) over \( \mathbb{Z}_2^r \) by
\[
S = \left( \bigcup_{f = f_s}^{\left\lceil \frac{r-m'}{2} \right\rceil - 1} 2^{\min(f+2,r-f-1)+\min(m', \max(0, r-2f-3)) - k} \right) \bigcup_{i = 0}^{\max(0, 2^{r-2f-3-m'} - 1)} \left\{ 2^{f+3+m'} i + q'2^{f+m'} + t' \right\}
\]

where all constants are integers between 0 and \( r \) inclusive, \( f_s \leq \left\lceil \frac{r-m'}{2} \right\rceil \) and \( m' \geq k \). The number of elements of the multiset \( S \) equals
\[2^{r-f_s-k}.
\]

**Proof.** When \( f_s \geq \left\lceil \frac{r-m'}{2} \right\rceil - 1 \) this result, with the help of Lemma 5, is trivial to check. Let us assume now that \( f_s \leq \left\lceil \frac{r-m'}{2} \right\rceil - 2 \). We consider two cases. The first case is when \( m' = 0 \) and \( r \) is odd, or \( m' \leq 1 \) and \( r \) is even. Then the number of elements of \( S \) is:
\[
\#S = 2^{\left\lceil \frac{r}{2} \right\rceil - k} + \sum_{f = f_s}^{\left\lceil \frac{r}{2} \right\rceil - 1} 2^{\min(f+2,r-f-1)+\min(m', \max(0, r-2f-3))-k+\max(0,r-2f-3-m')} = 2^{\left\lceil \frac{r}{2} \right\rceil - k} + \sum_{f = f_s}^{\left\lceil \frac{r}{2} \right\rceil - 1} 2^{f+2+m'-k+r-2f-3-m'}
\]
\[
= 2^{\left\lceil \frac{r}{2} \right\rceil - k} + \sum_{f = f_s}^{\left\lceil \frac{r}{2} \right\rceil - 1} 2^{-f-1-k}.
\]
We use now the formula for the sum of a geometric series:
\[
\#S = 2^{\left\lceil \frac{r}{2} \right\rceil - k+1} + 2^{r-f_s-k-1} \frac{1-2^{(-1)\left\lceil \frac{r}{2} \right\rceil - f_s}}{1-2} = 2^{\left\lceil \frac{r}{2} \right\rceil + 1} + 2^{r-f_s-k} \left( 1 - 2f_s+1-\left\lceil \frac{r}{2} \right\rceil \right) = 2^{\left\lceil \frac{r}{2} \right\rceil} + 2^{r-f_s-k} - 2^{\left\lceil \frac{r}{2} \right\rceil} = 2^{r-f_s-k}.
\]
Let us now consider the case where \( m' > 0 \) if \( r \) odd, or \( m' > 1 \) when \( r \) even. The same sum becomes:
\[
\#S = 2^{r-2f-3-m'+f+2+m'-k} = 2^{r-f-k-1}.
\]
Proof. 

\[
\begin{align*}
Z & = 2^{r+m'} \sum_{f = f_s}^{r-m'} - k 2^{r+2+\min(m', r-2f-3) - k + \max(0, r-2f-3-m')} \\
& = 2^{r+m'} \sum_{f = f_s}^{r-2} - k 2^{r+2+m'-k+r-2f-3-m'} \\
& = 2^{r+m'-k} + \sum_{f = f_s}^{r-2} 2^{r-f-k-1}.
\end{align*}
\]

We use once again the formula for the sum of a geometric series, which produces

\[
\# S = 2^{r+m'-k} + 2^{r-f_s-k} - 2^{r+m'-k+1} = 2^{r-f_s-k}.
\]

\[\square\]

In the proof of the next lemma we will use variables analogous to those we presented in Corollary 4. Before proceeding further, let us introduce one new notation that we will employ frequently:

\[m^* = m' - k,\]

where we should note that \(m^* \geq 0\) since \(m' \geq k\).

Before starting to prove Lemma 7, let us note first that it is not superseded by the earlier mentioned result of Marshall and Ramage \([23]\). Furthermore, we do not see a way to employ their proof technique to obtain this lemma—even when \(v = r\) and \(d = 0\). It is because, at the very beginning, they constraint solutions to equivalence classes that are over ring \(\mathbb{Z}_{2^r-1}\). For \(n = 2\) this right away limits the divisibility they may obtain to \(2^r-1\), which is less than Lemma 7 produces.

**Lemma 7.** Let \(P(x) = a_x x^2 + b_x x + c\) and \(Q(y, h) = a_y y^2 + b_y y + 2^{r-d} h\). Then for any \(d \leq v \leq r\) when we work over \(\mathbb{Z}_{2^r}\), it holds that:

\[
2^{v+d} \mid \# \left\{ (x, y, h) : x \in \bigcup_{j=0}^{2^r-1} \{ l_x + 2^{r-v} j \}, y \in \bigcup_{j=0}^{2^r-1} \{ l_y + 2^{r-v} j \}, h \in \bigcup_{j=0}^{2^r-1} \{ j \}, P(x) = Q(y, h) \right\}
\]

for any \(l_x, l_y\).

**Proof.** Depending on its constants, \(P\) may fall into category a), b) or c) as per Corollary 4. We will also consider \(Q\) to be in one of those categories depending to which of them the \(a_y y^2 + b_y y\) part of \(Q\) belongs. We will go through all possible pairings of those categories for \(P\) and \(Q\) and proof the result for each of them. Let us notice though that if \(P\) is in category b), we could treat it just as being in category a) but with taking its \(m'\) (or \(m'_x\) as we will call it) to be bigger by 1, but not bigger than \(r\). The same goes for \(Q\). Therefore category b) can be easily “reduced” to category a) and in the rest of the proof it is sufficient if we only consider \(P\) and \(Q\) to be in categories either a) or c).

1. Both \(P\) and \(Q\) are in category a).

The image of \(P\) is

\[
2^{m'_x-k} \bigcup_{i=0}^{2^r-m'_y-1} \left\{ 2^{m'_x i} + c' \right\}
\]

whereas the image of \(Q\) is

\[
2^{m'_y-k} \bigcup_{i=0}^{2^r-m'_y-1} \bigcup_{h=0}^{2^d-1} \left\{ 2^{m'_y i} + 2^{r-d} h \right\} = 2^{m'_y + \min(r-m'_y, d) - k} \bigcup_{i=0}^{2^r-r-1} \left\{ 2^{\min(m'_y, r-d) i} \right\}.
\]
where variables are defined in analogy to Corollary 4. If those two images have no common element we automatically obtain the required divisibility. Otherwise, their distinct common elements are all elements of the more sparse image, that is:

\[
2^{r - \max(m'_x, \min(m'_y, r - d)) - 1} \bigcup_{i=0}^{\max(m'_x, \min(m'_y, r - d) - 1)} \left\{ 2^{\max(m'_x, \min(m'_y, r - d))} i + g' \right\},
\]

where \( g' = 0 \) or \( c' \) depending on value of \( \max(m'_x, \min(m'_y, r - d)) \). There is \( 2^{r - \max(m'_x, \min(m'_y, r - d))} \) of those elements, and each of them has occurrences. This gives the size of the whole overlap to be

\[
2^{r - \max(m'_x, \min(m'_y, r - d))} 2^{m'_x - k} 2^{m'_y + (r - m'_y, d) - k} = 2^{\min(r - m'_x, r - \min(m'_y, r - d)) + \min(r - m'_y, d) + m'_x + m'_y}
\]

\[
= 2^{\min(v - m'_x + \min(v - m'_y, d), v - m'_y + d) + m'_x + m'_y}
\]

\[
= 2^{\min(2v, v + d + m'_y)},
\]

which produces the desired divisibility.

2. \( P \) is in category c) and \( Q \) is in category a).

The image of \( P \) is

\[
\left( \bigcup_{f=0}^{\left\lceil \frac{r - m'_x}{2} \right\rceil - 1} 2^{\min(f + 2, r - f - 1) + \min(m'_x, \max(0, r - 2f - 3)) - k} \bigcup_{i=0}^{\frac{\max(0, 2^{r - 2f - 3} - m'_x - 1)}{2^{2f + 3 + m'_x}}} \left\{ 2^{2f + 3 + m'_x} i + q' 2^{2f + m'_x} \right\} \right)
\]

\[
\bigcup 2^{\left\lceil \frac{r - m'_x}{2} \right\rceil - k} \{ t' \},
\]

and the image of \( Q \) is, once again,

\[
2^{\min(r, m'_y + d) - k} \bigcup_{i=0}^{\max(m'_y, r - d) - 1} \left\{ 2^{\min(m'_y, r - d)} i \right\}.
\]

The image of \( P \) consists of \( \left\lceil \frac{r - m'_x}{2} \right\rceil \) linear slices (one per value of \( f \)) and then the slice for \( \{ t' \} \), which we can take to have a period of \( 2^t \). If the images of \( P \) and \( Q \) have no common element, we automatically get the result. When the contrary is true, let us first assume that there is a common element between the two images at a slice

\[
\left\{ 2^{2f_0 + 3 + m'_x} i + q' 2^{2f_0 + m'_x} + t' \right\},
\]

for certain \( f_0 \). Let us consider the following cases:

2.1. \( \min(m'_y, r - d) \geq 2f_0 + 1 + m'_x \)

Under this condition only elements in that particular slice for \( f_0 \) may be common for the two images. Let \( \min(m'_y, r - d) = 2f_0 + 1 + m'_x + h \) for certain \( h \geq 0 \), which also automatically means that \( \min(r, m'_y + d) - k = 2f_0 + 1 + m'_x + h + d - k \). When \( h \leq 2 \) the whole slice is common. Then, starting at \( h = 2 \), whenever \( h \) increases by 1 the part of the slice for \( f_0 \) that is common is halved. By Lemma 5, the number of elements in the whole \( f_0 \) slice equals
$2^r - f_0 - k - 1$, and the size of whole overlap is the number of common elements in the slice for $f_0$ multiplied by the number of occurrences of each distinct element in the image of $Q$. Therefore the size of the intersection is

$$2^r - f_0 - k - 1 \cdot 2^{\min \left( (-h, 0) \cdot 2^m + d + k \right)} = 2^r - f_0 - k - 1 + \min \left( 2 - h, 0 \right) + 2f_0 + m_x + h + d - k$$

which has the desired divisibility.

### 2.2. $\min(m'_y, r - d) \leq 2f_0 + m'_x$

If $\min(m'_y, r - d) \geq m'_x$, then we can write that $\min(m'_y, r - d) = 2f_s + m'_x + h$ for certain $f_s \leq f_0$ and $0 \leq h \leq 1$. Otherwise, we have that $\min(m'_y, r - d) = k + h$ for certain $h < m'_x - k$, and we set $f_s = 0$. Now the common elements for both images that are in the image of $P$ are:

$$\left\{ \left\{ f \in \mathbb{F}\right\} \cup \left\{ \frac{r - m'_x}{2} \right\} - k \left\{ t' \right\} \right\}$$

that is, all slices for $f = f_s$ and higher orders. Each element in this part of the $P$ image will be multiplied $2^{\min \left( r, m'_y + d \right)} - k$ times, as there are that many elements in $Q$ image equal to it. We know from Lemma 6 that there is $2^r - f_s - k$ elements in the image of $P$ that are common. Let us do the multiplication considering the cases on $\min(m'_y, r - d)$ we described earlier. First when $\min(m'_y, r - d) = 2f_s + m'_x + h, 0 \leq h \leq 1$

$$2^r - f_s - k \cdot 2^{\min \left( r, m'_y + d \right)} - k = 2^r - f_s - k + 2f_s + m'_x + h + d - k = 2^v + d + f_s + h + m'_x,$$

and now when $\min(m'_y, r - d) = k + h, 0 \leq h < m'_y - k, f_s = 0$

$$2^r - f_s - k \cdot 2^{\min \left( r, m'_y + d \right)} - k = 2^r - k + h + d - k = 2^v + d + h.$$

This gives us the desired divisibility in both cases.

Finally we need to consider the scenario when the common element between both images is $\left\{ t' \right\}$, and there are no other different common elements. This means that

$$\min(m'_y, r - d) > 2^{\left\lceil \frac{r - m'_x}{2} \right\rceil - 1} - m'_x$$

therefore

$$\min(m'_y + d, r) = r + h$$

for certain $h = 0$ or $1$ depending on parity of $r - m'_x$. In this case the number of common elements is:

$$2^\left\lceil \frac{r + m'_x}{2} \right\rceil - k \cdot 2^{\min \left( r, m'_y + d \right)} - k = 2^\left\lceil \frac{r + m'_x}{2} \right\rceil - k + r + h + d - 1 + h - k = 2^v + d + h - 1 + \left\lceil \frac{v + m'_x}{2} \right\rceil.$$

If $h = 1$ (i.e., $r - m'_x$ is odd) this has the required divisibility. Otherwise, we know that $v + m'_x$ has to be even, since $r - m'_x$ is. If $v \geq 1$ this gives the desired divisibility, and when $v = 0$ the whole lemma becomes trivial.
3. \( P \) is in category a) and \( Q \) is in category c).

The image of \( P \) is

\[
2^{m'_x - k} \bigcup_{i=0}^{2^{r-m'_x} - 1} \left\{ 2^{m'_x i} + c' \right\}.
\]

When it comes to the image of \( Q \), for \( d = 0 \) it would be just an image of \( a_y y^2 + b_y y \), which consists of slices as we know them from Corollary 4:

\[
\left( \left\lfloor \frac{r-m'_x - d}{2} \right\rfloor - 1 \right) \bigcup_{f=0}^{2^{min(f+2,r-f-1)+min(m'_y,\max(0,r-2f-3))}-k} \bigcup_{i=0}^{\max(0,2^{r-2f-3-m'_y}-1)} \left\{ 2^{2f+3+m'_y i} + q'2^2f+m'_y + t' \right\}
\]

\[
= \left( \left\lfloor \frac{r-d-3-m'_y}{2} \right\rfloor - 1 \right) \bigcup_{f=0}^{2^{min(f+2,r-f-1)+min(m'_y,\max(0,r-2f-3))}-k} \bigcup_{i=0}^{\max(0,2^{r-2f-3-m'_y}-1)} \left\{ 2^{2f+3+m'_y i} + q'2^2f+m'_y + t' \right\}
\]

When \( d > 0 \), each of those slices is “affected” by the slice \( 2^{r-d}h \), which has granularity \( 2^{r-d} \). If an affected slice already has at least that granularity, then each of its elements has just \( 2^d \) more occurrences. Otherwise, we obtain a slice with \( 2^{r-d} \) period, where each element has number of occurrences equal to number of all elements in the affected slice. In effect the image of \( Q \) is:

\[
\left( \left\lfloor \frac{r-d-3-m'_y}{2} \right\rfloor - 1 \right) \bigcup_{f=0}^{2^{min(f+2,r-f-1)+min(m'_y,\max(0,r-2f-3))}-k} \bigcup_{i=0}^{\max(0,2^{r-2f-3-m'_y}-1)} \left\{ 2^{2f+3+m'_y i} + q'2^2f+m'_y + t' \right\}
\]

\[
= \left( \left\lfloor \frac{r-d-3-m'_y}{2} \right\rfloor - 1 \right) \bigcup_{f=0}^{2^{min(f+2,r-f-1)+min(m'_y,\max(0,r-2f-3))}-k} \bigcup_{i=0}^{\max(0,2^{r-2f-3-m'_y}-1)} \left\{ 2^{2f+3+m'_y i} + q'2^2f+m'_y + t' \right\}
\]

Basing on Lemmas 5 and 6, we can say that a slice for any given \( f \) in \( Q \)’s image has \( 2^{r+d-f-k-1} \) elements, and the number of elements in union of slices for a set \( f = f_s \), all higher \( f \)'s, and the \( \{ 2^{r-d}h + t' \} \) slice, equals \( 2^{r+d-f-k} \).

If the images of \( P \) and \( Q \) have no common elements, we automatically get the result. Now let us assume that they have a common element at some slice

\[
\left\{ 2^{2f_0+3+m'_y i} + q'2^{f_0+m'_y} + t' \right\}
\]

(i.e. \( f_0 \leq \left\lfloor \frac{r-d-3-m'_y}{2} \right\rfloor - 1 \)). If \( m'_x \geq 2f_0 + 1 + m'_y \), then only elements in that particular slice may be common for the images. Let \( m'_x = 2f_0 + 1 + m'_y + h \) for certain non-negative \( h \). When \( h \leq 2 \) then the whole slice is common. Then, starting at \( h = 2 \), whenever \( h \) increases by 1, the part of
the slice that is common is halved. Due to Lemma 5, the number of elements in whole slice equals \(2^{r-f_0-k-1}\), and the number of common elements is:

\[
2^{m'_x-k}2^{r+d-f_0-k-1}2^{\min(-(h-2),0)} = 2^{2f_0+1+m'_y+h-k+r+d-f_0-k-1+\min(2-h,0)}
\]

\[
= 2^{f_0+m'_y+r+d-k+\min(2,h)} = 2^{f_0+m'_y+\min(2,h)+v+d},
\]

which gives the desired divisibility.

Now let us assume that the images have a common element at some slice

\[
\left\{2^{r-d}h_0 + q'2^{f_0+m'_y'} + t'\right\}
\]

(i.e. \(\left\lfloor \frac{r-d-m'_y}{2} \right\rfloor - 1 \geq f_0 \geq \left\lfloor \frac{r-d-3-m'_y}{2} \right\rfloor\)). If \(m'_x \geq 2f_0 + 1 + m'_y\), then only elements in that particular slice may be common for the images. Let \(m'_x = 2f_0 + 1 + m'_y + h\) for certain non-negative \(h\). When \(m'_x \leq r - d \iff 2f_0 + 1 + m'_y + h \leq r - d \iff h \leq r - d - 1 - 2f_0 - m'_y\) then the whole slice is common. Then, starting at \(h = r - d - 1 - 2f_0 - m'_y\), whenever \(h\) increases by 1 then the part of the slice that is common is halved. We know that the number of elements in whole slice equals \(2^{r-d-f_0-k-1}\), and the number of common elements is:

\[
2^{m'_x-k}2^{r+d-f_0-k-1}2^{\min(-(h-(r-d-1-2f_0-m'_y)),0)} = 2^{2f_0+1+m'_y+h-k+r+d-f_0-k-1+\min(r-d-1-2f_0-m'_y-h,0)}
\]

\[
= 2^{f_0+m'_y+r+d-k+\min(r-d-1-2f_0-m'_y,h)} = 2^{f_0+m'_y+\min(r-d-1-2f_0-m'_y,h)+v+d},
\]

which again gives the desired divisibility.

Let us consider now a case when \(m'_x \leq 2f_0 + m'_y',\) i.e. where more than one slice form \(Q\) is common with \(P\). If \(m'_x \geq m'_y\) then we can write that \(m'_x = 2f_s + m'_y + h\) for certain \(f_s < f_0\) and \(h \leq 1\). Otherwise we have that \(m'_x = k + h\) for certain \(h < m'_y - k\), and we set \(f_s = 0\).

Now the common elements for both images that are in the image of \(Q\) are:

\[
\bigcup_{f=f_s}^{h_{max}} \left\lfloor \frac{r-d-3-m'_y}{2} \right\rfloor \bigcup_{f=f_s}^{h_{max}} \left\lfloor \frac{r-d-3-m'_y}{2} \right\rfloor 2^{\min(f+2,r-f-1)+\min(m'_y,\max(0,r-2f-3))-k+d} \bigcup_{i=0}^{\max(0,2^{r-2f-3-m'_y-1})} \left\{2^{2f+3+m'_y} + q'2^{f+m'_y} + t'\right\}
\]

\[
\bigcup_{f=f_s}^{h_{max}} \left\lfloor \frac{r-d-3-m'_y}{2} \right\rfloor 2^{r-f-k-1} \bigcup_{h=0}^{2^d-1} \left\{2^{r-d}h + q'2^{f+3+m'_y} + t'\right\} \bigcup_{h=0}^{2^d-1} \left\{\frac{r-\min(2f,k)}{2}-k\right\} \bigcup_{h=0}^{2^d-1} \left\{\frac{2^d-k}{2}h + t'\right\},
\]

that is, all slices for \(f = f_s\) and higher orders. Each element in this part of the \(Q\) image will be multiplied \(2^{m'_x-k}\) times, as there are that many elements in \(P\) image equal to it. We know basing on Lemma 6 that there are \(2^{r+d-f_s-k}\) elements in \(Q\) image that are common. Let us do the multiplication considering the cases on \(m'_x\) we described earlier. First when \(m'_x = 2f_s + m'_y + h,\) \(h \leq 1\)

\[
2^{r+d-f_s-k}2^{m'_x-k} = 2^{r+d+f_s-k+h+m'_y} = 2^{f_s+h+m'_y+d+v}
\]

and now when \(m'_x = k + h,\) \(0 \leq h < m'_y - k,\) \(f_s = 0\)

\[
2^{r+d-f_s-k}2^{m'_x-k} = 2^{r-k+k+h-k+d} = 2^{h+d+v}.
\]

This gives the desired divisibility in both cases.
Finally we need to consider the case in which the only common slice between the images is \( \{2^{r-d}h + t'\} \). This means that

\[
m'_z > 2 \left( \frac{r - d - m'_y}{2} \right) - 1 \right) + m'_y
\]

therefore

\[
m'_z = r - d - 1 + h
\]

for certain \( h \geq 0 \) or \( h \geq 1 \) depending on the parity of \( r - d - m'_y \). In that case the number of common elements is:

\[
C = 2^{\min(d, r - m'_y)}2^{m'_z - k}2^{\left\lfloor \frac{r - \min(d, r - m'_y)}{2} \right\rfloor} - k
\]

Let us consider two sub-cases, first when \( v > d \) giving:

\[
C = 2^{r-d-1+h-k}2^{\left\lfloor \frac{r + \min(d, r - m'_y)}{2} \right\rfloor} - k
\]

\[
= 2^{\min(d, h, 1) - 1}2^{\left\lfloor \frac{v + \min(m'_y, v - d)}{2} \right\rfloor}
\]

If \( h \geq 1 \) this gives the required divisibility. When \( h = 0 \) it means that \( r - d - m'_y \) is even and therefore also that \( v - d + \min(m'_y, v - d) \) is even. Because \( v > d \) it means that \( v - d + \min(m'_y, v - d) \geq 2 \), which also results in required divisibility. Let us consider now the case for \( v = d \), starting over from the initial formula for the size of the intersection:

\[
C = 2^{\min(v, r - m'_y)}2^{m'_z - k}2^{\left\lfloor \frac{r + \min(v, r - m'_y)}{2} \right\rfloor} - k
\]

\[
= 2^{v + \left\lfloor \frac{v + \min(m'_y, v - d)}{2} \right\rfloor} = 2^v + 2^v = 2^v,
\]

which also has the desired divisibility.

4. Both \( P \) and \( Q \) are in category c).

The image of \( P \) is

\[
\left( \left\lfloor \frac{r - m'_y}{2} \right\rfloor - 1 \right) \bigcup_{f=0}^{2^\min(f+2, r-f-1)+\min(m'_y, \max(0, r-2f-3))} 2^\max(0, 2^{r-2f-3-m'_y}) - k \bigcup_{i=0}^{m'_z} \left\{ 2^{2f+3+m'_y} + 2^f + m'_y \right\}
\]

\[
\bigcup 2^{\left\lfloor \frac{r + m'_y}{2} \right\rfloor - k} \{0\}
\]

and the image of \( Q \), once again, is:

\[
\left( \left\lfloor \frac{r-d-3-m'_y}{2} \right\rfloor - 1 \right) \bigcup_{f=0}^{2^\min(f+2, r-f-1)+\min(m'_y, \max(0, r-2f-3))} 2^\max(0, 2^{r-2f-3-m'_y}) - k + d \bigcup_{i=0}^{m'_z} \left\{ 2^{2f+3+m'_y} + q'_y 2^{2f+m'_y} + t'_y \right\}
\]

\[
\bigcup \left( \left\lfloor \frac{r-d-m'_y}{2} \right\rfloor - 1 \right) \bigcup_{f=0}^{2^{r-f-1}} \bigcup_{h=0}^{2^f-1} \left\{ 2^{r-d}h + q'_y 2^{2f+m'_y} + t'_y \right\} \bigcup \bigcup_{h=0}^{2^f-1} 2^{\left\lfloor \frac{r + \min(d, r - m'_y)}{2} \right\rfloor} - \left\{ 2^{r-d}h + t'_y \right\}
\]

We could take \( q'_x = 1 \) and \( t'_x = 0 \) (which allowed us to omit them in the formula), since when faced with \( P(x) = Q(y, h) \) we can first divide both sides by \( q'_x \) and then subtract \( \frac{t'_x}{q'_x} \), which appropriately also adjusts \( q'_y \) and \( t'_y \) (both \( q'_x \) and \( q'_y \) are guaranteed to be odd). If there are no common elements
between the two images then we are automatically done. Let us now assume that there is an
overlap, i.e. that there is at least one common element between the images. Our approach is to go
through all possible classes of overlaps between pairs of slices, and then for any such overlap we
will show either that it has the required divisibility, or that there have to be some more overlaps
that together with this one have that divisibility. We will also never count the same overlaps more
than once.

4.a. First let us assume there is a common element between certain slice for \( f_x \) and a slice for
\( f_y \leq \left\lceil \frac{r-d-3-m_y'}{2} \right\rceil - 1 \). Let us go through cases:

4.a.1. \( 2f_x + m_x' \geq 2f_y + m_y' \):

Then the number of common elements between those two slices is the number of elements in the slice \( f_x \) multiplied by the number of occurrences of each distinct element in the slice \( f_y \), that is:

\[
\begin{align*}
2^{r-f_x-1} & \cdot \min(f_y+2, r-f_y-1) + \min(m_y', \max(0, r-2f_y-3))-k+d \\
& = 2^{r-f_y-1} + 2f_y + 2 + m_y' - k + d = 2^{v+d + m_y' - f_x + f_y + 1}
\end{align*}
\]

since \( f_y \leq \left\lceil \frac{r-d-3-m_y'}{2} \right\rceil - 1 \). If \( f_x \leq m_y' + f_y + 1 \) then the common part of those two slices already has the desired divisibility. Therefore let us assume now, that there is a pair of slices that overlap, for which \( f_x \geq m_y' + f_y + 2 \). The slice for \( f_y \) has a “period” of \( 2^{2f_x + 3 + m_y'} \). If that slice overlaps with the slice

\[
\{2^{2f_y + m_y'}\} \subseteq \{2^{2(m_y'+m_y'+1+h)}\}
\]

(for certain even \( h \geq 0 \)), then it also overlaps with all other slices attainable from it by
shifting by a multiple of the \( 2^{2f_x + 3 + m_y'} \) period. Therefore the slice for \( f_y \) overlaps with slices

\[\{0\} \text{ and } \{2^{2f_y + 3 + m_y'+m_y'+1+h}\}\]

for all even \( h \geq -m_y' - m_y' - 1 \). This means that the slice for \( f_y \) overlaps with slices \( \{0\} \) and \( \{2^{2f_y + m_y'}\} \) for any \( f_x \) such that

\[
2f_x + m_x' \geq 2f_y + 3 + m_y' \iff f_x \geq \left\lceil \frac{2f_y + 3 + m_y' - m_y'}{2} \right\rceil.
\]

Let us count the number of common elements between the slice for \( f_y \) and the union of the just-mentioned slices. Using Lemma 6 we know the size of that union is

\[
2^{v} - \left\lceil \frac{2f_y + 3 + m_y' - m_y'}{2} \right\rceil - k,
\]

whereas the number of occurrences of each distinct element in the slice for \( f_y \) is \( f_y + 2 + m_y' - k + d \), which gives:

\[
2^{-\left\lceil \frac{2f_y + 3 + m_y' - m_y'}{2} \right\rceil - k + f_y + 2 + m_y' - k + d} = 2^{-\left\lceil \frac{2f_y + 3 + m_y' - m_y'}{2} \right\rceil + f_y + 2 + m_y' + d} = 2^{v+d - \left\lceil \frac{m_y' - m_y' - 1}{2} \right\rceil},
\]

that produces the desired divisibility.

4.a.2. \( 2f_x + m_x' < 2f_y + m_y' \):

Now the number of common elements between the slices is the number of elements in the slice \( f_y \), multiplied by the number of occurrences of each distinct element in the slice \( f_x \), that is:

\[
D = 2^{r-d-1}\min(f_x+2, r-f_x-1) + \min(m_x', \max(0, r-2f_x-3))-k.
\]

Now we need to consider the following two subcases:
4.a.2.1. $r - 2f_x - 3 - m'_x \geq 0$:

$$D = 2^{v+d-f_y-k-1+f_x+2+m'_s-k-d} = 2^{v+d+m'_s-f_y+f_x+1}.$$  

This case is analogous to the case we already considered—just $d$ shows up in a different place. If $f_y \leq m'_s + f_x + 1$, then the common part of those two slices already has the desired divisibility. Therefore let us assume now that there is a pair of slices that overlap, for which $f_y \geq m'_s + f_x + 2$. The slice for $f_x$ has a “period” of $2^{2f_x+m'_s}$. If that slice overlaps with the slice

$$\{q'_s 2^{f_x+m'_s} + t'_y\} = \{q'_s 2^{(m'_s+f_x+2h)+m'_s} + t'_y\} = \{q'_y 2^{2f_x+3+m'_s+m'_y+1+h} + t'_y\}$$

(for certain even $h \geq 0$), then it also overlaps with all other slices attainable from it by shifting by a multiple of the $2^{2f_x+m'_s}$ period. Therefore the slice for $f_x$ overlaps with slices

$$\{t'_y\} \text{ and } \{q'_y 2^{2f_x+m'_s} + t'_y\},$$

for all even $h \geq -m'_s - m'_y - 1$. This means that the slice for $f_x$ overlaps with slices $\{t'_y\}$ and $\{q'_y 2^{2f_x+m'_s} + t'_y\}$, for any $f_y$ such that

$$2f_y + m'_y \geq 2f_x + 3 + m'_x \Leftrightarrow f_y \geq \frac{2f_x + 3 + m'_x - m'_y}{2}.$$  

Let us count the number of common elements between the slice for $f_x$ and the union of the just-mentioned slices. Basing on Lemma 6 we know the size of that union is

$$2^{-\left\lfloor \frac{2f_x+3+m'_s-m'_y}{2} \right\rfloor - k+d}$$

(overlaps with slices $\{t'_y\}$ and $\{q'_y 2^{2f_x+m'_s} + t'_y\}$ for any $f_y$ such that

$$2f_y + m'_y \geq 2f_x + 3 + m'_x \Leftrightarrow f_y \geq \frac{2f_x + 3 + m'_x - m'_y}{2}.$$  

which also produces the desired divisibility.

4.a.2.2. $0 > r - 2f_x - 3 - m'_x$

$$D = 2^{r-f_y-k-1+f_x+2+m'_s-k-d} = 2^{v-f_y+2+d}.$$  

In this case $f_x = \left\lfloor \frac{r-m'_s}{2} \right\rfloor - 1 = \left\lfloor \frac{v-m'_s}{2} \right\rfloor - 1$, $f_y \leq \left\lfloor \frac{r-3-m'_s}{2} \right\rfloor - 1 = \left\lfloor \frac{v-m'_s-3}{2} \right\rfloor - 1$. Let us substitute them into the equation (we take worst case for $f_y$), obtaining:

$$D = 2^{v-\left\lfloor \frac{v-m'_s}{2} \right\rfloor - \left\lfloor \frac{v-m'_s-3}{2} \right\rfloor + d} = 2^{v+d+h}$$

for certain non-negative $h$.

4.b. Now let us assume there is a common element between certain slices for $f_x$ and $\left\lfloor \frac{r-d-m'_s}{2} \right\rfloor - 1 \geq f_y$.

4.b.1. $2f_x + 3 + m'_x \geq r - d$:

In this case the number of common elements between the two slices is the number of elements in the slice for $f_x$ multiplied by the number of occurrences of each distinct element in the slice $f_y$, that is:

$$2^{r-f_x-k-1}2^{r-f_y-k-1} = 2^{2v-f_y-f_y-2}.$$  

There are one or two possible values of $f_y$, depending whether $r - d - m'_y$ is even or odd.
4.b.1. First let us take \( f_y = \left\lfloor \frac{r-d-m'_y}{2} \right\rfloor - 1 \), in which case above expression equals
\[
2^{v-f_x-\left\lfloor \frac{r-d-m'_y}{2} \right\rfloor - 1}.
\]
If \( f_x \leq v - d - \left\lfloor \frac{r-d-m'_y}{2} \right\rfloor - 1 \) we automatically get the required divisibility. Therefore let us assume, now, that there is a pair of slices that overlap, for which \( f_x \geq v - d - \left\lfloor \frac{r-d-m'_y}{2} \right\rfloor \). The slice for \( f_y \) has a “period” of \( 2^{r-d} \). If that slice overlaps with slice
\[
\left\{ 2^{2f_x+m'_y} \right\} = \left\{ 2^{\left\lfloor v-d-\left\lfloor \frac{r-d-m'_y}{2} \right\rfloor +m'_y+g \right\}} = \left\{ 2^{r-d+m'_y+m'_y+s} \right\}
\]
(for certain \( g \geq 0 \), \( s \geq -1 \)), then it also overlaps with all other slices attainable from it by shifting by a multiple of the \( 2^{r-d} \) period.
If \( m'_y = m'_y = 0 \) and \( s = -1 \) (i.e. \( r-d-m'_y \) is odd) it means that the only overlapping slice is \( \left\{ 2^{r-d+i} + 2^{r-d-1} \right\} \), as \( \left\{ 2^{r-d} + q'_y 2^{r-d-1} + t'_y \right\} \) doesn’t intersect with any other slice for any \( h \). In this case \( 2f_x + m'_x = r - d - 1 \leftrightarrow f_x = \left\lfloor \frac{r-d-m'_y-1}{2} \right\rfloor \), but the ceiling means nothing as \( r-d-m'_x \) is even, since \( r-d-m'_y \) is odd and \( m'_y = m'_x \) due to \( m_y = m_x = 0 \). The number of common elements between those two slices is therefore:
\[
2^{r-\left\lfloor \frac{r-d-m'_y-1}{2} \right\rfloor - k - 1 + \left\lfloor \frac{r-d-m'_y}{2} \right\rfloor - k} = 2^{2v-\left\lfloor \frac{r-d-1}{2} \right\rfloor - \left\lfloor \frac{r-d}{2} \right\rfloor - 1} = 2^{v+d-1}
\]
Yet in this case we claim that also the slice \( \left\{ 2^{r-d} + t'_y \right\} \) overlaps with all the slices for \( f_x + 1 \) and higher. First, the slice for \( f_y \) is \( \left\{ 2^{r-d} + q'_y 2^{r-d-1} + t'_y \right\} \) in this case, and the slice for \( f_x \) is \( \left\{ 2^{r-d+i} + 2^{r-d-1} \right\} \), and they overlap - which means that \( 2^{r-d} \mid t'_y \) (\( q'_y \) is guaranteed to be odd). Any slice for any higher \( f_x = f_x + c + 1, c \geq 0 \) is \( \left\{ 2^{r-d+i} + 2^{r-d+c} \right\} \), and therefore it has to overlap with the slice \( \left\{ 2^{r-d} + t'_y \right\} \). Let us count the size of this overlap:
\[
2^{r-\left( \left\lfloor \frac{r-d-m'_y-1}{2} \right\rfloor + 1 \right) - k} = 2^{v-d-1}
\]
Together with the \( 2^{v+d-1} \) we obtained earlier, this gives the required divisibility.
Now let us suppose that \( m'_y \geq 1 \) or \( m'_y \geq 1 \) or \( s \geq 0 \). Then the slice for \( f_y \) overlaps with some slice \( \left\{ 2^{r-d+z_0} \right\} \) for certain \( z_0 \geq 0 \), which means that it also overlaps with slice \( \{0\} \), and we are in the case 4.e.

4.b.1.2. Let us consider now the second possible value of \( f_y \), that is \( f_y = \left\lfloor \frac{r-d-3-m'_y}{2} \right\rfloor \), and in this case \( r-d-m'_y \) is odd (otherwise this value of \( f_y \) would equal the value we already considered). Now the size of the common part of the two slices that overlap is:
\[
2^{v-f_x-f_y-2} = 2^{2v-f_x-\left\lfloor \frac{r-d-3-m'_y}{2} \right\rfloor - 2}.
\]
If \( f_x \leq v - d - \left\lfloor \frac{r-d-3-m'_y}{2} \right\rfloor - 2 \) this gives the required divisibility. Let us assume now it does not, and we have \( f_x \geq v - d - \left\lfloor \frac{r-d-3-m'_y}{2} \right\rfloor - 1 \). In this case the slice for \( f_y \) overlaps with slice:
\[
\left\{ 2^{2f_x+m'_y} \right\} = \left\{ 2^{\left\lfloor v-d-\left\lfloor \frac{r-d-3-m'_y}{2} \right\rfloor - 1 \right\rfloor +m'_y+g} \right\} = \left\{ 2^{2v-2d-r+d+2k+1+m'_y+m'_y+g} \right\} = \left\{ 2^{r-d+1+m'_y+m'_y+g} \right\}
\]

49
for certain non-negative even \( g \). Now, also the slice for \( f_y \) overlaps with all the slices above for all possible \( g \), therefore the common part is:

\[
2^{r - \left( v - d - \left\lfloor \frac{r - d - 3 - m_x'}{2} \right\rfloor - 1 \right)} - k = 2^{v + d},
\]

which gives the required divisibility.

4.b.2. \( 2f_x + 3 + m_x' < r - d \):

In this case the number of common elements between the two slices is the number of elements in the slice for \( f_y \) multiplied by the number of occurrences of each distinct element in the slice \( f_x \), that is:

\[
D = 2^{r + d - f_y - k - 1} 2^{\min(f_x + 2, r - f_x - 1) + \min(m_x', \max(0, r - 2f_x - 3)) - k}
\]

Now we need to consider the following two cases:

4.b.2.1. \( r - 2f_x - 3 - m_x' \geq 0 \):

\[
D = 2^{r + d - f_y - k - 1 + f_x + 2 + m_x' - k + d} = 2^{v + d + m_x' - f_y + f_x + 1}.
\]

This case behaves exactly as the already considered case 4.a.2.1.

4.b.2.2. \( 0 > r - 2f_x - 3 - m_x' \):

\[
D = 2^{r + d - f_y - k - 1 + r - f_x - k - 1} = 2^{2v - f_y - f_x - 2 + d}.
\]

In this case \( f_x = \left\lfloor \frac{r - m_x'}{2} \right\rfloor - 1 = \left\lfloor \frac{v - m_x^*}{2} \right\rfloor - 1, f_y \leq \left\lfloor \frac{r - m_y^* - d}{2} \right\rfloor - 1 = \left\lfloor \frac{v - m_y^* - d}{2} \right\rfloor - 1. \]
Let us substitute them into the equation (we take worst case for \( f_y \))

\[
D = 2^{2v - \left\lfloor \frac{v - m_x^*}{2} \right\rfloor - \left\lfloor \frac{v - m_y^* - d}{2} \right\rfloor + d}.
\]

If either \( m_x^*, m_y^* \) or \( d \) is greater than 0 or \( v \) is even, then this gives the required divisibility. Otherwise, we obtain

\[
D = 2^{2v - 2\left\lfloor \frac{v}{2} \right\rfloor},
\]

and \( r - k \) is odd (since \( v \) is odd). Therefore

\[
2^{2f_x + m_x'} = 2^{2f_x + m_y'} = 2^{2\left\lfloor \frac{r + d}{2} \right\rfloor - 2 + k} = 2^{r - 1}.
\]

This means that the two overlapping slices we are looking at are both \( \{2r - 1\} \). It also means that \( t_y' = 0 \), and that also slices containing \( \{0\} \) overlap. The number of common elements for the \( \{0\} \) slices is

\[
2^{\left\lfloor \frac{r + d}{2} \right\rfloor - k} = 2^{\left\lfloor \frac{v}{2} \right\rfloor},
\]

and let us note that

\[
2^{2v - 2\left\lfloor \frac{v}{2} \right\rfloor} + 2^{2\left\lfloor \frac{v}{2} \right\rfloor + 1} = 2^v.
\]

This gives the desired divisibility.

4.c. Now let us consider the cases where the slices that overlap are for certain \( f_x \) and for \( \{2r - d + t_y'\} \). Once again, we need to look at two subcases:

4.c.1. \( 2f_x + 3 + m_x' \geq r - d \):

The number of common elements is the number of elements in slice for \( f_x \) multiplied by the number of occurrences of each element in the slice \( \{2r - d + t_y'\} \).

\[
2^{r - f_x - k - 1} 2^{\frac{r - \min(d + m_x^*, v)}{2} - k} = 2^{v - f_x - 1 + \frac{r - \min(d + m_x^*, v) - 2k}{2}} = 2^{v - f_x - 1 + \frac{v + \min(d + m_x^*, v)}{2}}.
\]
If $f_x \leq \left\lfloor \frac{v + \min(d + m_x^*, v)}{2} \right\rfloor - d - 1$, then we obtain the required divisibility. Let us take now that $f_x \geq \left\lfloor \frac{v + \min(d + m_x^*, v)}{2} \right\rfloor - d$. The slice \( \{2^{r-d}h + t'_y\} \) has a common element with the slice

\[
2^{2f_x + m_y^*} = \left\{ 2^{\left\lfloor \frac{v + \min(d + m_y^*, v)}{2} \right\rfloor - d + m_x^*} \right\} = \left\{ 2^{r-d+\min(m_y^*, v-d)+m_x^*} \right\}
\]

(for certain $g \geq 0, s \geq -1$), and so it likewise overlaps with all other slices attainable from it by shifting by a multiple of the $2^{r-d}$ period. If $m_y^* = 0, s = -1$ (i.e. $v + \min(d + m_y^*, v)$ is odd) and $\min(m_y^*, v-d) = 0$, it means that the only overlapping slice is

\[
\{2^{r-d+2i} + 2^{r-d-1}\},
\]

since

\[
\{2^{r-d}h + t'_y\}
\]
doesn’t intersect with any other slice for any $h$. In this case $2f_x + m_y^* = r - d - 1 \iff f_x = \left\lfloor \frac{r-d-m_y^*-1}{2} \right\rfloor$. The number of common elements between those two slices is:

\[
2^r \left[ \frac{r-d-m_y^*-1}{2} \right] - k + 1 + 2^r \left[ \frac{v + \min(d + m_y^*, v)}{2} \right] - k = 2^r \left[ \frac{v + \min(d + m_y^*, v)}{2} \right] - 1.
\]

Because $v + \min(d + m_y^*, v)$ is odd, it means that $\min(d + m_y^*, v) = d + m_y^*$, $\min(m_x^*, v-d) = m_x^*$, and therefore $m_y^* = 0$. Also, because $v + d + m_y^*$ is odd, we get that $v - d + m_y^* = r - d + m_x^*$ is odd, which means that $m_y^*$ has different divisibility by 2 than $r - d$. Additionally $v - d - m_y^* = r - d - m_y^*$ is odd too. Therefore, if we take $f'_y = \left\lceil \frac{r-d-m_y^*}{2} \right\rceil - 1$, the slice for it will be

\[
\{2^{r-d}h + q_y^* 2^{r-d-1} + t'_y\}
\]

(we know that $d + m_y^* \leq r$ as $\min(d + m_y^*, v) = d + m_y^*$).

First, the slice for (our original) $f_y$ is \( \{2^{r-d}h + t'_y\} \) in this case, and the slice for $f_x$ is \( \{2^{r-d+2i} + 2^{r-d-1}\} \), and they overlap—which means $2^{r-d} \mid t'_y$ and $2^{r-d-1} \mid t'_y$. Slice for any higher $f_x^\prime = f_x + c + 1, c \geq 0$ equals \( \{2^{r-d+4+2i} + 2^{r-d+2i} + 2^{r-d+1+2i}\} \), and therefore it has to overlap with slice \( \{2^{r-d}h + q_y^* 2^{r-d-1} + t'_y\} \). Let us count the size of this overlap:

\[
2^r \left( \frac{r-d-m_y^*}{2} + 1 \right) - k = 2^r \left( \frac{r-d-m_y^*}{2} - k \right) = 2^{r+d-1}
\]

Together with the $2^{r+d-1}$ we obtained earlier, this gives the required divisibility. Let us note that this case is different from case 4.b.1.1 with $s = -1$ and $m_x^* = m_y^* = 0$, as here the slice \( \{2^{r-d+2i} + 2^{r-d-1}\} \) overlaps with \( \{2^{r-d}h + t'_y\} \), whereas there the slice \( \{2^{r-d+2i} + 2^{r-d-1}\} \) overlapped with \( \{2^{r-d}h + q_y^* 2^{r-d-1} + t'_y\} \).

Now let us suppose that $\min(m_y^*, v-d) \geq 1$ or $m_x^* \geq 1$ or $s \geq 0$. Then the slice \( \{2^{r-d}h + t'_y\} \) overlaps with some slice \( \{2^{r-d+z_0}\} \) for certain $z_0 \geq 0$, which means that it also overlaps with slice \( \{0\} \), and we are in the case 4.f.

4.c.2. $2f_x + 3 + m_x^* < r - d$:

The number of common elements is the number of elements in slice \( \{2^{r-d}h + t'_y\} \) multiplied by number of occurrences of each element in the slice for $f_x$:

\[
D = 2^r \left[ \frac{v + \min(d + m_x^*, v)}{2} \right] - k + d 2^{r-d-1} + \min(m_x^*, v-d) = 2^r \left[ \frac{r+d-m_x^*}{2} \right] - k.
\]

Let us consider the following two cases:
4.c.2.1. \( r - 2f_x - 3 - m'_x \geq 0 \): 

\[
D = 2^{\left\lfloor \frac{r - \min(d + m'_y, v)}{2} \right\rfloor - k + d + f_x + 2 + m'_x - k} = 2^{\left\lfloor \frac{r - \min(d + m'_y, v)}{2} \right\rfloor + d + f_x + 2 + m'_x}.
\]

If \( \min(d + m'_y, v) = v \) we automatically have the required divisibility. Let us assume now the other case, when the above becomes

\[
D = 2^{\left\lfloor \frac{v + d + m'_y}{2} \right\rfloor + d + f_x + 2 + m'_x}.
\]

If

\[
\left\lfloor \frac{v + d + m'_y}{2} \right\rfloor + d + f_x + 2 + m'_x \geq v + d \Leftrightarrow f_x \geq v - \left\lfloor \frac{v + d + m'_y}{2} \right\rfloor - 2 - m'_x
\]

\[
\Leftrightarrow f_x \geq \left\lfloor \frac{v - d - m'_y}{2} \right\rfloor - 2 - m'_x \Leftrightarrow f_x \geq \left\lfloor \frac{r - d - m'_y}{2} \right\rfloor - 2 - m'_x
\]

then we automatically obtain the required divisibility. Let us assume now that

\[
f_x \leq \left\lfloor \frac{r - d - m'_y}{2} \right\rfloor - 3 - m'_x.
\]

In this case, there is a certain \( f_y \) with which slice the slice for our \( f_x \) overlaps. Because the slice for \( f_x \) overlaps with \( \{2^{r-d+h+t'_y}\} \), and has a period of \( 2^{2f_x+m'_x+3} \), then it also contains any element of the form

\[
\left\{ 2^{2f_x+m'_x+3} i + t'_y \right\} = 2^{\left\lfloor \frac{r - d - m'_y}{2} \right\rfloor - 3 - 2m'_x - h + m'_x i + t'_y}
\]

\[
= 2^{\left\lfloor \frac{r - d - m'_y}{2} \right\rfloor - 3 - m'_x - h + k i + t'_y i + t'_y}
\]

for certain \( h \geq -1 \) and any \( i \). The maximum possible \( f_y \) equals \( \left\lfloor \frac{r - d - m'_y}{2} \right\rfloor - 1 \), and its slice contains

\[
\left\{ 2^{\left\lfloor \frac{r - d - m'_y}{2} \right\rfloor - 2 + m'_y} + t'_y \right\} = 2^{\left\lfloor \frac{r - d - m'_y}{2} \right\rfloor - 2 + m'_y + k + t'_y}.
\]

Therefore the slices for our \( f_x \) and for the maximum possible \( f_y \) overlap, which means we are in the already-considered case 4.b.2.1—we just approached it here from the “other end”.

4.c.2.2. \( 0 > r - 2f_x - 3 - m'_x \)

\[
D = 2^{\left\lfloor \frac{r - \min(d + m'_y, v)}{2} \right\rfloor - k + d + r - f_x - k - 1} = 2^{v + \left\lfloor \frac{r - \min(d + m'_y, v)}{2} \right\rfloor - d - f_x - 1}.
\]

In this case \( f_x = \left\lfloor \frac{r - m'_y}{2} \right\rfloor - 1 = \left\lfloor \frac{v - m'_x}{2} \right\rfloor - 1 \), let us substitute:

\[
D = 2^{v + d + 1 + \left\lfloor \frac{v + \min(d + m'_y, v)}{2} - \frac{v - m'_x}{2} \right\rfloor}
\]

This gives the desired divisibility unless \( m'_y = m'_x = d = 0 \) and \( v \) is odd, in which case we have

\[
D = 2^{v - 1}.
\]
Let us take \( f_y \) to be maximal, i.e. \( f_y = \left\lceil \frac{r-m'_y}{2} \right\rceil - 1 \). When \( v \) is odd and \( m'_y = m'_x = 0 \), then also \( r - k \) is odd, and additionally

\[
2^2 f_y + m'_y = 2^2 f_x + m'_x = 2^{2 \left\lceil \frac{r-k}{2} \right\rceil - 2 + k} = 2^{r-1}.
\]

Because \( \{ 2' h + t'_y \} \) overlaps with the slice for \( f_x \), it means that \( t'_y = 2^{r-1} \). Therefore also the slice \( \{ 0 \} \) overlaps with the slice for the maximal \( f_y \), i.e. \( \{ 2' h + 2^2 f_y + m'_y + t'_y \} \).

Owing to symmetry (which is here due to \( d = 0 \)), the size of that overlap also equals \( 2^{v-1} \), which together with the earlier overlap gives the desired \( 2^v \).

4.d. Let us consider now the case where the slices that overlap are \( \{ 0 \} \) and a certain slice for \( f_y \) where \( f_y \leq \left\lceil \frac{r-d-3-m'_y}{2} \right\rceil - 1 \). This case is very similar to 4.c.2.1. The number of common elements is the number of elements in the slice \( \{ 0 \} \) multiplied by the number of occurrences of each element in slice for \( f_y \), that is

\[
2 \left\lceil \frac{r-m'_y}{2} \right\rceil - k \min(f_y + 2, r - f_y - 1) + \min(m'_y, \max(0, r - 2 f_y - 3)) - k + d = 2 \left\lceil \frac{r-m'_y}{2} \right\rceil - k + f_y + 2 + m'_x + d,
\]

since \( f_y \leq \left\lceil \frac{r-d-3-m'_y}{2} \right\rceil - 1 \).

If

\[
f_y \geq \left\lceil \frac{r-m'_x}{2} \right\rceil - 2 - m'_y,
\]

then we automatically obtain the required divisibility. Let us assume now that

\[
f_y \leq \left\lceil \frac{r-m'_x}{2} \right\rceil - 3 - m'_y.
\]

In this case, there is a certain \( f_x \) with which slice the slice for our \( f_y \) overlaps. Because the slice for \( f_y \) overlaps with \( \{ 0 \} \), and has the period of \( 2^{2 f_y + m'_y + 3} \), then it also contains any element of the form

\[
\{ 2^2 f_x + m'_y + 3 \} = \left\{ 2 \left\lceil \frac{r-m'_x}{2} \right\rceil - 3 - m'_y - h + m'_x \right\} = \left\{ 2 \left\lceil \frac{r-m'_x}{2} \right\rceil - 3 - h + m'_x + k \right\}
\]

for certain \( h \geq -1 \) and any \( i \). The maximum possible \( f_x \) equals \( \left\lceil \frac{r-m'_x}{2} \right\rceil - 1 \), and its slice contains

\[
\left\{ 2 \left\lceil \frac{r-m'_x}{2} \right\rceil - 2 + m'_y \right\} = \left\{ 2 \left\lceil \frac{r-m'_x}{2} \right\rceil - 2 + m'_y + k \right\}.
\]

Therefore the slice for our \( f_y \) and for the maximal \( f_x \) overlap, which means we are in the already-considered case 4.a—we just approached it here from the “other end”.

4.e. Let us assume now that there is a common element between the slice \( \{ 0 \} \) and a certain slice for \( \left\lceil \frac{r-d-3-m'_y}{2} \right\rceil - 1 \geq f_y \geq \left\lceil \frac{r-d-3-m'_y}{2} \right\rceil \).

The slice for \( f_y \) is

\[
\left\{ 2^{r-d} h + q'_y 2^{2 f_y + m'_y} + t'_y \right\} = \left\{ 2^{r-d} h + q'_y 2^{2 \left\lceil \frac{r-d-m'_y}{2} \right\rceil - g + m'_y + t'_y \right\}
\]

\[
= \left\{ 2^{r-d} h + q'_y 2^{r-d-s} + t'_y \right\},
\]

where \( g = 1 \) or \( g = 2 \), and \( s = 1 \) or \( s = 3 \) (when \( r - d - m'_y \) odd) or \( s = 2 \) (when \( r - d - m'_y \) even). Because \( \{ 0 \} \) overlaps with \( \left\{ 2^{r-d} h + q'_y 2^{r-d-s} + t'_y \right\} \) it means that \( 2^{r-d} | q'_y 2^{r-d-s} + t'_y \), and that the second slice is just \( \left\{ 2^{r-d} h \right\} \).
Any slice
\[ \left\{ 2^2 f_x + 3 + m'_s i + 2^2 f_x + m'_s \right\} \]
overlaps with the slice
\[ \left\{ 2^r - d h \right\} \]
whenever
\[ 2 f_x + m'_s \geq r - d \iff f_x \geq \left\lfloor \frac{r - d - m'_s}{2} \right\rfloor. \]

Let us count number of common elements of those overlaps:
\[ 2^r \left\lfloor \frac{r - d - m'_s}{2} \right\rfloor - k 2^r \left( \left\lfloor \frac{r - d - m'_s}{2} \right\rfloor - y \right) - k - 1 = 2^{v - \left\lfloor \frac{v - d - m'_s}{2} \right\rfloor} - \left\lfloor \frac{v - d - m'_s}{2} \right\rfloor - 1 + g. \]

It gives the desired divisibility unless \( g = 1, m'_y = m'_s = 0 \) and \( v - d \) is odd. Yet in that case let us notice that the slice for \( f'_x = \left\lfloor \frac{r - d - m'_s}{2} \right\rfloor - 1 = \left\lfloor \frac{v - d}{2} \right\rfloor - 1 \) and the slice \( \left\{ 2^r - d h + t'_y \right\} \) are respectively:
\[ \left\{ 2^2 f'_x + 3 + m'_s i + 2^r - d - 1 \right\} \quad \text{and} \quad \left\{ 2^r - d h + 2^r - d - 1 \right\} \]

\( (q'_y \) is always odd, in this case \( s = 1 \) and therefore \( t'_y = 2^r - d - 1 \). This means that those two slices overlap, which indicates this is the same case as 4.c.1 for \( m'_x = m'_y = 0 \) and \( v + \min(d + m'_x, v) \) being odd.

4.f. Finally let us consider the case where the slice \( \{0\} \) overlaps with the slice \( \left\{ 2^r - d h + t'_y \right\} \).

This case is very similar to the previous one, yet different. Because those two slices overlap it means that \( 2^r - d | t'_y \), and in fact the second slice is just \( \left\{ 2^r - d h \right\} \).

Any slice
\[ \left\{ 2^2 f_x + 3 + m'_s i + 2^2 f_x + m'_s \right\} \]
overlaps with the slice
\[ \left\{ 2^r - d h \right\} \]
whenever
\[ 2 f_x + m'_s \geq r - d \iff f_x \geq \left\lfloor \frac{r - d - m'_s}{2} \right\rfloor. \]

Let us count number of common elements of those overlaps:
\[ 2^r \left\lfloor \frac{r - d - m'_s}{2} \right\rfloor - k 2^r \left( \left\lfloor \frac{r - d - m'_s}{2} \right\rfloor - y \right) - k - 1 = 2^{v - \left\lfloor \frac{v + m + d + m'_x, v}{2} \right\rfloor} - \left\lfloor \frac{v + m + d + m'_x, v}{2} \right\rfloor - 1 + g. \]

If \( \min(d + m'_x, v) = v \), it is easy to check this gives the required divisibility. Let us assume the opposite case, obtaining
\[ = 2^{v + m + d + m'_x, v} + \left\lfloor \frac{v + d + m'_s}{2} \right\rfloor. \]

This gives the required divisibility, unless \( m'_s = m'_x = 0 \) and \( v + d \) is odd. Yet in that case let us notice that the slices for \( f'_x = \left\lfloor \frac{r - d - m'_s}{2} \right\rfloor - 1 = \left\lfloor \frac{v - d}{2} \right\rfloor - 1 \) and \( f'_y = \left\lfloor \frac{r - d - m'_s}{2} \right\rfloor - 1 = \left\lfloor \frac{v - d}{2} \right\rfloor - 1 \) are respectively:
\[ \left\{ 2^2 f'_x + 3 + m'_s i + 2^r - d - 1 \right\} \quad \text{and} \quad \left\{ 2^r - d h + 2^r - d - 1 \right\} \]

\( (q'_y \) is always odd), which means those two slices overlap. And this means that this is the same case as 4.b.1.1 for \( m'_s = m'_y = 0 \) and \( r - d - m'_y \) odd, and it was already considered.
To sum up, we showed that whenever there is any overlap, then either it is divisible by $2^{v+d}$, or there are some additional overlaps which sum together to that divisibility. We also never counted the same common elements of images $P$ and $Q$ more than once, which can be seen via comparison of cases that refer to each other.

\[\square\]

**Corollary 2. (restated)**
Let $P(x) = a_x x^2 + b_x x + c_x$ and $Q(y, h) = a_y y^2 + b_y y + c_y + 2^{r-d} h$ where $d \leq r$. Then for any $v, q \in [d, r]$, when we work over $\mathbb{Z}_{2^r}$ it holds that:

$$2^{\min(v, q) + d} \mid \# \left\{ (x, y, h) : x \in \bigcup_{j=0}^{2^v-1} \{ l_x + 2^{-v} j \}, y \in \bigcup_{j=0}^{2^q-1} \{ l_y + 2^{-q} j \}, h \in \bigcup_{j=0}^{2^r-1} \{ j \}, P(x) = Q(y, h) \right\},$$

for any $l_x, l_y$.

**Proof.** Let us take $M = \max(v, q)$ and $m = \min(v, q)$. Then we can split the larger of the two domains into $2^{M-m}$ slices each of some form

$$\bigcup_{j=0}^{2^m-1} \{ l + 2^{-m} j \}$$

for appropriately shifted $l$'s. Next we can use Lemma 7 $2^{M-m}$ times, for each of those smaller slices of the larger domain separately. Then we notice that each time we obtain that the size of the intersection is divisible by $2^{n+d}$, and the divisibility of a sum is not smaller than the smallest of the divisibilities of its components. Finally, to obtain any $c_x$ and $c_y$ we wish, we can just choose $c = c_x - c_y$ in Lemma 7, and then add $c_y$ to both sides of the equation. \[\square\]

When proving the base case of our main theorem we have come against a specific multiset that a polynomial we will have may potentially intersect with. The following lemma contributed to the divisibility of the size of such an intersection.

**Lemma 8.** Let us work over $\mathbb{Z}_{2^r}$. Let $P(x) = a_x x^2 + b_x x + c$ with $x$ being constrained to domain $x \in \bigcup_{j=0}^{2^v-1} \{ l_x + 2^{-v} j \}$ for certain $l_x$ and $v \leq r$. Let $S$ be the following multiset:

$$S = \left( \bigcup_{i=0}^{2^v-1} \bigcup_{f_s=0}^e f_s \bigcup_{s=0}^{2^{v-\epsilon}-1} \{ 2^{v-\epsilon} i + 2^{v-f_s} (2s + 1) \} \right) \bigcup \left( \bigcup_{i=0}^{2^r-1} (v+1) \{ 2^{v} \} \right),$$

where $\epsilon \leq v$. The number of elements of the intersection (understood as a “multiplicative” intersection as described above) of the multiset $S$ and the image of $P$ is divisible by

$$2^{v+\min(v, \lceil \frac{r}{2} \rceil)}.$$

**Proof.** The multiset $S$ can be also written as

$$S = \left( \bigcup_{f_s=0}^e f_s \bigcup_{s=0}^{2^{v-\epsilon}-1} \{ 2^{v-\epsilon} i + 2^{v-f_s} (2s + 1) \} \right) \bigcup \left( \bigcup_{i=0}^{2^v-1} \bigcup_{f_s=v-\epsilon}^e f_s \bigcup_{s=0}^{2^{v-\epsilon}-1} \{ 2^{v-\epsilon} i \} \right) \bigcup \left( \bigcup_{i=0}^{2^r-1} (v+1) \{ 2^{v} \} \right),$$

where we used the formula for the sum of an arithmetic-geometric series on $\bigcup_{f_s=v-\epsilon}^e f_s \bigcup_{s=0}^{2^{v-\epsilon}-1} \{ 2^{v-\epsilon} i \}$. From now on we will refer to set $S$ as presented in the last of the written above forms.

$P$ may belong to one of the categories a), b) or c) as per Corollary 4. Let us go through cases on those categories:

55
1. \( P \) is in category a).

The image of \( P \) is

\[ 2^{m'_x-k} - k \sum_{i=0}^{2^{v-m'_x-1}} \left\{ 2^{m'_s i} + c' \right\} \]

If it has no common elements with \( S \) we are automatically done. When the contrary is true, let us first assume that a common element is in a slice \( \{2^{r-v} + f_s (2s + 1)\} \) for certain \( f_s \). Let us consider two cases

1.a. \( m'_x > r - v + f_s \)

In this case only the elements belonging to the slice for \( f_s \) may be in the intersection. The size of the common part equals the number of all elements in the \( P '\)‘s image multiplied by the number of occurrences of each distinct element in the slice for \( f_s \), giving

\[ 2^v f_s 2^e = f_s 2^{r+v}, \]

which has the required divisibility.

1.b. \( m'_x \leq r - v + f_s \)

In this case the of \( P \) intersects with all elements of all slices for any \( f'_s \) such that \( m'_x \leq r - v + f'_s \), and also of the slice \( \{2^{r-v} \} \). The size of that overlap is the number of all those elements multiplied by the number of occurrences of each distinct element from the image of \( P \). The number of elements in the slices for all \( f_s \geq m^*_x \), and the last slice \( \{2^{r-v} \} \), is

\[ 2^v ((m^*_x + 1)2^{v-m^*_x} - (v - e + 1)2^e + (v - e + 1)2^e) = (m^*_x + 1)2^{v+v-m^*_x} \]

(via use of the formula for an arithmetic-geometric series sum). Therefore the size of the intersection is

\[ (m^*_x + 1)2^{v+v-m^*_x} 2^{m'_s-k} = (m^*_x + 1)2^{v+e}, \]

which has the required divisibility.

Finally we need to consider the scenario in which the common elements are in the slice \( \{2^{r-v} \} \), and there are no common elements in any other slice of \( S \). This means that

\[ m'_x = r - e + h \]

for certain \( h \geq 0 \). In this case the size of the intersection equals to number of all elements of the image of \( P \) multiplied by the number of occurrences of each distinct element of the slice \( \{2^{r-v} \} \), giving

\[ 2^v (v - e + 1)2^e = (v - e + 1)2^{v+e}, \]

which has the required divisibility.

2. \( P \) is in category b).

This case can be reduced to the previous one by taking \( m'_x \) to be bigger by 1, but not bigger than \( r \).

3. \( P \) is in category c).

Because \( P \) is of type c) we know that \( m'_x \geq 2k + h_x \) for certain \( h_x \geq 0 \) (compare with \( a' \) from Corollary 4), and also \( m'_x < r \). Therefore

\[ 2k + h_x < r \iff 2(r - v) + h_x < r \iff v > \left\lceil \frac{r + h_x}{2} \right\rceil, \]

56
which means that it will be sufficient to show the divisibility by $2^{e+\lceil e/2 \rceil}$. In this case the image of $P$ is
\[
\left( \sum_{f_x=0}^{r-m'_t} \right)^{-1} \sum_{f_x=0}^{2^{\min(f_x+2x-v-f_x-1) + \min(m'_x, \max(0, v-2f_x-3)) - k}} \left( \prod_{i=0}^{\max(0, 2^{r-2f_x-3-m'_x-1})} \left( 2^{2f_x+3+m'_x+q}2^{2f_x+m'_x+1} \right) \right)
\]
whereas $S$ is, once again,
\[
\left( \sum_{f_x=0}^{r-e-1} \right)^{-k} \sum_{f_x=0}^{2^{v-f_x-1}} \left( \prod_{s=0}^{2^{v-f_x+(2s+1)}} \right) \left( \prod_{i=0}^{2^{v-e}+1} \left( 2^{e+i} \right) \right).
\]
If there is no overlap between $S$ and the image of $P$, then we automatically obtain the desired result. Let us assume now that there is an overlap. Our strategy will be to go through all possible cases of such overlaps and then show that either the overlap has required divisibility on its own, or that there have to be some additional overlaps that together with the initial one have the desired divisibility. We will also never use any overlap more than once to complement an overlap not having sufficient divisibility on its own. Let us proceed to the cases:

3.a. There is an overlap between the slices $\{t'\}$ and $\{2^{-e}i\}$.

In this case the slice $\{2^{-e}i\}$ overlaps with all slices for $f_x$ such that $2f_x + m'_x \geq r-e \iff f_x \geq \left\lfloor \frac{r-e-m'_x}{2} \right\rfloor$. The size of that overlap is the number of elements in slices for all such $f_x$ and $\{t'\}$, multiplied by the number of occurrences of each distinct element in the slice $\{2^{-e}i\}$. Using Lemma 6 this gives
\[
2^{r-e} \left\lfloor \frac{r-e-m'_x}{2} \right\rfloor - k = (v-e+1)2^{e} \left\lfloor \frac{r-e-m'_x}{2} \right\rfloor - k = (v-e+1)2^{e+\lceil e/2 \rceil}.
\]
The above has the required divisibility unless $h_x = e = 0$, $r$ is odd, and $v$ is even. Yet, it is not a sole overlap when that happens. The pairs of slices for any $f_x$ such that $2f_x + m'_x < o(t')$ and $f_x$ such that $r-v+f_x = 2f_x + m'_x$ also overlap, since $2^{r-v+f_x+1}|t'$ due to $f_x \leq v-e-1$ and $2^{r-v}|t'$. Because we require
\[
2f_x + m'_x < o(t') \iff 2f_x < o(t') - m'_x
\]
and
\[
f_x = 2f_x + m'_x < v-e \iff 2f_x < v-e,
\]
let us denote $\min(o(t') - m'_x, v-e-m'_x)$ as $M$ so that $\left\lfloor \frac{M}{2} \right\rfloor - 1$ will be the limit of our sum. Let us count now the size of those pairwise overlaps. We will compute it for general $h_x, e$ etc. first, since that computation will be also useful for us later:
\[
\sum_{f_x=0}^{[\frac{M}{2}]^{-1}} 2^{r-f_x-k-1} f_x 2^e = 2^{e} \sum_{f_x=0}^{[\frac{M}{2}]^{-1}} (2f_x + m'_x) 2^{v-f_x-1}
\]
\[
= 2^{e} \left( 2^{\left\lfloor \frac{M}{2} \right\rfloor - 2 + m'_x} 2^{v-\left\lfloor \frac{M}{2} \right\rfloor - 1} - m'_x 2^{v-1} - 2 \left( 2^{\left\lfloor \frac{M}{2} \right\rfloor - 1} - 2^{v-2} \right) \right),
\]
There is an overlap between the slice $f$. This gives the desired divisibility. Let us use now our assumptions (i.e. $h_x = e = 0$, $r$ is odd, and $v$ is even, $t' = 0$ due to $e = 0$), which continue the calculation as:

$$= (v + g + 2)2^{|\frac{v}{r}|} = (v + 3)2^{|\frac{v}{r}|},$$

since $g = 1$ owing to $M = \min(o(t') - m_x, v - e - m_x) = \min(2v - r, 2v - r)$ being odd. Let us add it now to the earlier-found overlap (for the $\{2^{r-e}i\}$ slice):

$$(v + 3)2^{|\frac{v}{r}|} + (v + 1)2^{|\frac{v}{r}|} = (v + 2)2^{|\frac{v}{r}|} + 1.$$

This gives the desired divisibility.

3.b. There is an overlap between the slice $\{t'\}$, and a slice for certain $f_s \leq v - e - 1$. The slice for $f_s$ is

$$\{2^{r-v+f_s+1}s + 2^{r-v+f_s}\},$$

and for it to overlap with $\{t'\}$ it is necessary that

$$t' = 2^{r-v+f_s+1}j + 2^{r-v+f_s}$$

for certain $j$. Let us also notice that in this case the slice for $f_s$ overlaps with any slice $f_x'$ such that $2^{r-s} + m_x' \geq r - v + f_s + 1$, as any such slice is:

$$\left\{2^{2^{r-s}+m_x'}i + q't^{2^{r-s}+m_x'} + t'\right\} = \left\{2^{r-v+f_s+1+d+3}i + q'2^{r-v+f_s+1+d} + 2^{r-v+f_s+1}j + 2^{r-v+f_s}\right\},$$

for certain $d \geq 0$. The size of that whole overlap is the number of elements of all slices for $f_x' \geq \left\lfloor\frac{r-v+f_s+1-m_x}{2}\right\rfloor$ multiplied by the number of occurrences of each distinct element in the slice $f_s$, that is:

$$2^r \left\lfloor\frac{r-v+f_s+1-m_x}{2}\right\rfloor^{t'-2s} = f_s2^r \left\lfloor\frac{t'+1-m_x}{2}\right\rfloor = f_s2^r \left\lfloor\frac{t'+1-m_x}{2}\right\rfloor$$

This gives the required divisibility unless $f_s = v - 1$, $h_x = 0$ and $r$ is odd. In that unfortunate case, we get that $t' = 2^{r-1}$ and $e = 0$, and there is also an additional overlap “group”.

(where we used the formula for sum of the arithmetic-geometric series)

$$= 2^{r+1} \left( m_x^r 2^{v-1} + 2^r - \left( \frac{M}{2} - 2 + m_x^r \right) 2^{v-\left\lfloor\frac{v}{2}\right\rfloor - 1} - 2^{v-\left\lfloor\frac{v}{2}\right\rfloor + 1} \right)$$

$$= 2^{r+1} \left( m_x^r + 2 \right) 2^{v-1} - \left( \min(o(t') - k, v - e) + g - 2 \right) 2^{v-\left\lfloor\frac{v}{2}\right\rfloor - 1} - 2^{v-\left\lfloor\frac{v}{2}\right\rfloor + 1}$$

$$= 2^r \left( m_x^r + 2 \right) 2^v - \left( \min(o(t') - k, v - e) + g + 2 \right) 2^{v-\left\lfloor\frac{v}{2}\right\rfloor}$$

for certain $g = 0$ or 1 depending on the parity of $M$. The first element of this difference already has the required divisibility, so let us focus on the second one:

$$(\min(o(t') - k, v - e) + g + 2)2^e - \left\lfloor\frac{\min(o(t') - k, v - e - m_x)}{2}\right\rfloor$$

$$= (\min(o(t') - k, v - e) + g + 2)2^{e-\left\lfloor\frac{\min(o(t') - k, v - e - m_x)}{2}\right\rfloor}$$

Let us use now our assumptions (i.e. $h_x = e = 0$, $r$ is odd, and $v$ is even, $t' = 0$ due to $e = 0$), which continue the calculation as:

$$= (v + g + 2)2^{|\frac{v}{r}|} = (v + 3)2^{|\frac{v}{r}|},$$

since $g = 1$ owing to $M = \min(o(t') - m_x, v - e - m_x) = \min(2v - r, 2v - r)$ being odd. Let us add it now to the earlier-found overlap (for the $\{2^{r-e}i\}$ slice):

$$(v + 3)2^{|\frac{v}{r}|} + (v + 1)2^{|\frac{v}{r}|} = (v + 2)2^{|\frac{v}{r}|} + 1.$$
Let us take the maximal $f_x'$, i.e. $2f_x' + m_x' = r - 1$ ($r$ is odd, $h_x = 0 \Rightarrow m_x'$ is even), and look at its slice
\[
\left\{ 23f_x' + 3 + m_x' + q' 2^2 f_x' + m_x' + t', 2^2 f_x' + m_x' + t' \right\} = \left\{ q' 2^{r-1} + 2^{r-1} \right\} = \{0\}
\]
Therefore it overlaps with the slice $\{ 2^{r-e} i \} = \{0\}$ (since $e = 0$). We have that $f_x' = \frac{2r - r - 1}{2}$
and the size of that overlap is
\[
2^{r-\frac{2r-r-1}{2} - k-1} 2^e (v - e + 1) = (v + 1) 2^\frac{r-1}{2}.
\]
Let us add it to the earlier-found overlap:
\[
(v + 1) 2^\frac{r-1}{2} + f_x 2^e + \left\lfloor \frac{m_x'}{2} \right\rfloor = (v + 1) 2^\frac{r-1}{2} + (v - 1) 2^\left\lfloor \frac{r}{2} \right\rfloor = v 2^\left\lfloor \frac{r}{2} \right\rfloor.
\]
This gives the required divisibility.

3.c. There is an overlap between a slice for certain $f_x \leq \left\lfloor \frac{r - m_x'}{2} \right\rfloor - 1$ and the slice $\{ 2^{r-e} i \}$. The slice for $f_x$ is
\[
\left\{ 2^2 f_x + 3 + m_x' + q' 2^2 f_x + m_x' + t' \right\}
\]
and for it to overlap with the slice $\{ 2^{r-e} i \}$ it is necessary that
\[
t' = 2^{\min(2f_x + 3 + m_x', r-e)} j - q' 2^2 f_x + m_x'
\]
for certain $j$. Let us consider three sub-cases:

3.c.1. $r - e \leq 2f_x + m_x'$
   In this case we have $t' = 2^{r-e} j'$.
   for certain $j'$. It is easy to notice that the slice $\{ 2^{r-e} i \}$ overlaps with slice for any $f_x'$ such that $2f_x' + m_x' \geq r - e$ and with the slice $\{ t' \}$.
   Let us count the size of this overlap as a whole, which equals to number of all elements in this overlap from the image of P multiplied by number of occurrences of any distinct element in the slice $\{ 2^{r-e} i \}$.
\[
2^r \left\lfloor \frac{r - m_x'}{2} \right\rfloor - k 2^e (v - e + 1) = (v - e + 1) 2^e \left\lfloor \frac{m_x'}{2} \right\rfloor
\]
which gives the required divisibility unless $e = h_x = 0$, $v$ is even, and $r$ is odd. Yet, because in such a case we have that $\{ 2^{r-e} i \}$ intersects with $\{ t' \}$, it is a situation that we already considered in the case 3.a.

3.c.2. $2f_x + 3 + m_x' > r - e > 2f_x + m_x'$
   Now we have $t' = 2^{r-e} j - q' 2^2 f_x + m_x'$
   and $f_x = \left\lfloor \frac{r - e + m_x'}{2} \right\rfloor - 1$.

   Let us count the size of the overlap between the slice for $f_x$ and $\{ 2^{r-e} i \}$:
\[
2^{r-f_x - k-1} 2^e (v - e + 1) = (v - e + 1) 2^e \left\lfloor \frac{r - e + m_x'}{2} \right\rfloor + 1 - k-1 = (v - e + 1) 2^e \left\lfloor \frac{r - e + m_x'}{2} \right\rfloor.
\]
This gives the required divisibility unless $e = h_x = 0$, $v$ is even, and $r$ is odd, which we assume now. Therefore, we get $t' = 2^{r-1}$. Let us notice that the slice for $f_x'$ such that $r - v + f_x' = 2f_x + m_x' = r - 1$ is:
\[
\{ 2^{r-1} \}
\]
which overlaps with the slice $\{ t' \} = \{ 2^{r-1} \}$. This means that this is the case 3.b, which we already considered (we just arrived at it from another end).
3.c.3. \( r - e \geq 2f_x + 3 + m_x' \)

Now we have

\[
t' = 2^{2f_x + 3 + m_x'} j - q' 2^{2f_x + m_x'}.
\]

In this case the slice for \( f_x \) is

\[
\left\{ q2^{2f_x + 3 + m_x'} i + q' 2^{2f_x + m_x'} + t' \right\} = \left\{ q2^{2f_x + 3 + m_x'} i \right\}
\]

and it is easy to notice that it overlaps with all slices for \( f_x \) such that \( r - v + f_x \geq 2f_x + 3 + m_x' \) and with the slice \( \{ 2^{r-e} i \} \). The size of this overlap is the number of elements in the slices for those \( f_x \) multiplied by the number of occurrences of each distinct element in the slice for \( f_x \). The number of elements in the slices for all \( f_x \geq 2f_x + 3 + m_x' \), and the last slice \( \{ 2^{r-e} i \} \), is

\[
2^e (2f_x + 4 + m_x') 2^{v-2f_x-3-m_x'} - (v-e+1) 2^e + (v-e+1) 2^e = (2f_x + 4 + m_x') 2^{e+v-2f_x-3-m_x'}
\]

(via use of formula for arithmetic-geometric sequence sum), while the number of repetitions of any element in the slice for \( f_x \) is

\[
2^{\min(f_x, 2r-f_x-1)+\min(m_x', \max(0, r-2f_x-3))-k} = 2^{f_x+2+m_x'-k},
\]

since \( r \geq 2f_x + 3 + m_x' \). The size of the overlap is:

\[
(2f_x + 4 + m_x') 2^{e+v-2f_x-3-m_x'} 2^{f_x+2+m_x'-k} = (2f_x + 4 + m_x') 2^{e+v-f_x-1}
\]

Because \( f_x = \left\lceil \frac{r-e-m_x'}{2} \right\rceil - d \) for certain non-negative \( d \), we have

\[
= (v-e+1-2d) 2^{e+v-\left\lceil \frac{r-e-m_x'}{2} \right\rceil -1+d} = (v-e+1-2d) 2^{e+v-\left\lceil \frac{r-e-m_x'}{2} \right\rceil +d} = (v-e+1-2d) 2^{e+\left\lceil \frac{r-e-m_x'}{2} \right\rceil +d},
\]

which gives the required divisibility.

3.d. There is an overlap between a slice for certain \( f_x \leq \left\lceil \frac{r-m_x'}{2} \right\rceil - 1 \), and a slice for certain \( f_x \geq v - e - 1 \).

Let us consider following sub-cases:

3.d.1. \( 2f_x + m_x' \geq r - v + f_x + 1 \)

In this case \( 2^{2f_x + m_x'} = 2^{r-v+f_x+1+d} \) for certain \( d \geq 0 \). The slice for \( f_x \) is

\[
\left\{ q2^{2f_x + 3 + m_x'} i + q' 2^{2f_x + m_x'} + t' \right\} = \left\{ 2^{r-v+f_x+1+d} i + q' 2^{r-v+f_x+1+d} + t' \right\}.
\]

For it to overlap with the slice

\[
\left\{ 2^{r-v+f_x+1} j + 2^{r-v+f_x} \right\},
\]

it is necessary that

\[
t' = 2^{r-v+f_x+1} j + 2^{r-v+f_x}
\]

for certain \( j \). Let us also notice that in this case the slice for \( f_x \) overlaps with any slice \( f_x' \) such that \( 2f_x' + m_x' \geq r - v + f_x + 1 \) (if \( f_x \) was the smallest of them, then we would have \( d = 0 \) or \( d = 1 \)). That also includes an overlap with the slice \( \{ t' \} \). The size of that whole overlap is the number of elements of all slices for \( f_x' \geq \left\lceil \frac{r-v+f_x+1+m_x'}{2} \right\rceil \) multiplied by the number of occurrences of each distinct element in the slice \( f_x \), that is:

\[
2^{r-\left\lceil \frac{r-v+f_x+1+m_x'}{2} \right\rceil - k} f_x 2^e = f_x 2^{e+v-\left\lceil \frac{r+1-m_x'}{2} \right\rceil}
\]

60
The above gives the desired divisibility unless \( f_s = v - 1, h_x = 0, v \) is even, and \( r \) is odd, which we now assume. This gives us also \( e = 0 \). Because in this case the slice for \( f_s \) also overlaps with the slice \( \{ t' \} = \{ 2^r - 1 \} \), it means we are in the case 3.b, which we already considered.

3.d.2. \( 2f_x + m'_s = r - v + f_s \)

The slice for \( f_x \) is
\[
\left\{ 2^j f_x + 3 + m'_s i + q' 2^j f_x + m'_s + t' \right\} = \left\{ 2^{r-v} + f_x + 3 + q' 2^{r-v} + f_x + t' \right\}
\]
and the slice for \( f_s \) is
\[
\left\{ 2^{r-v} + f_s + 1 + 2^{r-v} + f_s \right\}.
\]
For those two slices to overlap it is necessary that
\[
t' = 2^{r-v} f_s + 1 j
\]
for certain \( j \) such that \( o(j) \leq v - f_s - 1 \). For any \( f'_s \) such that \( 2 f'_s + m'_s < o(t') \), and \( f'_s \) such that \( r-v + f'_s = 2 f'_s + m'_s \) and \( f'_s \leq v-e-1 \Leftrightarrow 2 f'_s + m'_s < r-e \), the slices for \( f'_s \) and \( f'_s \) overlap. Let us denote \( \min(o(t') - m'_s, r-e-m'_s) = \min(o(j) + f_s + 1 - m'_s, v-e-m'_s) \) by \( M \), and let us count the size of those overlaps:
\[
\sum_{f'_s=0}^{\left\lfloor \frac{M}{2} \right\rfloor -1} 2^{r-f'_s-k-1} f'_s, f'_s 2^e = 2^e \sum_{f'_s=0}^{\left\lfloor \frac{M}{2} \right\rfloor -1} (2 f'_s + m'_s) 2^{v-f'_s-1}
\]
\[
= 2^e \left( (2^{\left\lfloor \frac{M}{2} \right\rfloor} - 2 + m'_s) 2^{v-\left\lfloor \frac{M}{2} \right\rfloor -1} - m'_s 2^{v-1} - 2^v \left( 2^{\left\lfloor \frac{M}{2} \right\rfloor -1} - 2^{v-2} \right) \right)
\]
(\text{where we used the formula for sum of the arithmetic-geometric series})
\[
= 2^e + 1 \left( m'_s 2^{v-1} + 2^{v-1} - \left( 2^{\left\lfloor \frac{M}{2} \right\rfloor} - 2 + m'_s \right) 2^{v-\left\lfloor \frac{M}{2} \right\rfloor -1} - 2^v \left( 2^{\left\lfloor \frac{M}{2} \right\rfloor -1} - 2^{v-2} \right) \right)
\]
\[
= 2^{e+1} \left( (m'_s + 2) 2^{v-1} - (\min(o(j) + f_s + 1, v-e) + g) 2^{v-\left\lfloor \frac{M}{2} \right\rfloor -1} - 2^v \left( 2^{\left\lfloor \frac{M}{2} \right\rfloor -1} + 1 \right) \right)
\]
\[
= 2^{e+1} \left( (m'_s + 2) 2^{v-1} - \min(o(j) + f_s + 1, v-e + 1, v-e) 2^{v-\left\lfloor \frac{M}{2} \right\rfloor -1} - 2^v \left( 2^{\left\lfloor \frac{M}{2} \right\rfloor -1} + 1 \right) \right)
\]
for certain \( g = 0 \) or \( 1 \). The first element of this difference already has the required divisibility, so let us focus on the second one:
\[
(\min(o(j) + f_s + 1, v-e) + g + 2) 2^{e+v-\left\lfloor \frac{\min(o(j) + f_s + 1, v-e) + g + 2}{2} \right\rfloor}
\]
\[
= (\min(o(j) + f_s + 1, v-e) + g + 2) 2^{e-v} \left( \min(o(j) + f_s + 1, v-e + 1, v-e + 1, v-e + 1, v-e + 1) \right)
\]
The above has the required divisibility unless \( o(j) + f_s + 1 = v \) (i.e. \( o(t') = r \), \( e = h_x = 0 \), \( v \) is even, and \( r \) is odd, which we now assume. Yet due to that we get \( t' = 0 \), and therefore the slices \( \{ t' \} \) and \( \{ 2^{r-v} \} \) overlap. This means we land in the already-considered case 3.a.
3.d.3. \(2f_x + 3 + m'_x > r - v + f_s > 2f_x + m'_x\)

In this case we have

\[ f_x = \left\lfloor \frac{r - v + f_s - m'_x}{2} \right\rfloor - 1. \]

Let us count size of the overlap between those two slices:

\[ 2^{r-f_s-k-1}f_s 2^e = f_s 2^{e+r-\left\lfloor \frac{r - v + f_s - m'_x}{2} \right\rfloor +1-k-1} \]

\[ = f_s 2^e + \left\lfloor \frac{\alpha - m'_x + b s}{2} \right\rfloor \]

which gives the required divisibility, as \(f_s \leq v - 1\).

3.d.4. \(r - v + f_s \geq 2f_x + 3 + m'_x\)

For the slice

\[ \{2^{2f_x+3+m'_x} + q 2^{2f_x+m'_x} + t'\} \]

to overlap with the slice

\[ \{2^{r-v+f_s+1} + 2^{r-v+f_s}\} = \{2^{2f_x+4+m'_x+d} + 2^{2f_x+3+m'_x+d}\} \]

(for certain \(d \geq 0\)) it is necessary that

\[ t' = 2^{2f_x+3+m'_x} - q 2^{2f_x+m'_x} \]

in which case the slice for \(f_x\) is just

\[ \{2^{2f_x+3+m'_x}\} \]

and it is easy to notice that it overlaps with all slices for \(f'_s\) such that \(r - v + f'_s \geq 2f_x + 3 + m'_x\)

and also with the slice \(\{2^{-e}i\}\). Fortunately, we already considered such a scenario in the case 3.c.

\[ \square \]

**Corollary 3.** (restated)

Let us work over a ring \(\mathbb{Z}_2^r\). Let \(P(x) = a_xx^2 + b_xx + c\) with \(x\) being constrained to the domain \(x \in \bigcup_{j=0}^{2^r-1} \{l_x + 2^{-q}j\}\) for certain \(l_x\) and \(v \leq r\). Let \(S\) be the following multiset:

\[ S = \left( \bigcup_{i=0}^{2^r-1} f_s \bigcup_{s=0}^{2^r-f_s-1} \{2^{-e}i + 2^{r-v+fs' + (2s + 1)}\} \right) \cup \left( \bigcup_{i=0}^{2^r-1} (v + 1) \{2^{-e}i\} \right), \]

where \(e \leq \min(q,v)\). The number of elements of the intersection (understood as a “multiplicative” intersection) of the multiset \(S\) and the image of \(P\) is divisible by

\[ 2^{e+\min(q,v,\left\lfloor \frac{r}{2} \right\rfloor)}. \]

**Proof.** The proof is analogous to that of Corollary 2, but using Lemma 8 as the base.
8 Future work

As exemplified in Theorems 1 and 2, the solution spaces have a specific structure, built around cosets of ideals. This describes a certain kind of symmetry of the solutions around the unit circle, which, as mentioned, is significant for properties of the Z-function and may have applications in computational complexity. We are certain that a lot of this structure is still left to be discovered, especially extending Theorem 2 to polynomials of any degree and rings over general composite numbers is desirable. Theorem 1 shows that for \( \mathbb{Z}_m \) where \( m = p_1^{i_1}p_2^{i_2} \ldots p_k^{i_k} \), there are symmetries in multiple “dimensions” (which result from the use of Chinese remaindering), one per each \( p_i \). We speculate about possible symmetries beyond those given by the decomposition into local rings.

A different angle on the problem, mentioned earlier in the introduction, is provided by restricting the arguments to subsets of the domain, which elements are pairwise incongruent modulo a set prime ideal. This allows restriction of variables to, for example, \( \{0, 1\}^n \). This is studied very recently by Clark, Forrow and Schmitt [14], with the focus on lower-bounding the size of the gap between 0, and the second smallest solution number. Thanks to values we present in Table 15 we can experimentally see that results from [14] are not optimal for composite \( m \). For example, for a single polynomial over \( \mathbb{Z}_m \) having degree up to 2 and with variables not restricted to any subset of the ring, they say that the first gap is at least \( 2^{q(n-2)} \), where \( n \) is the number of variables of the polynomial. For \( q = 4 \) and \( n = 2 \) it gives 1 as minimum size of the gap, whereas the gap is already 8. For \( n = 3 \), their bound is 16, with the gap being 64. Therefore, there is a room for improvement and future research on establishing tighter bounds for this gap. Yet, encouraged by our experiments, we believe that even greater results may be obtained by focusing on the size of the last gap instead (i.e. the gap between the two largest possible numbers of solutions). If one would look at rings of size \( r = 2^q \) in Table 16, the guess could be, that the size of this gap is \( 2^{q-1}n \) when \( n \leq 2 \), and \( 2^{q(n-2)+2(q-1)} \) otherwise. Similar results look plausible for \( r = 3^r \), yet for higher primes a large gap already shows for \( n = 1 \), due to the degrees of the polynomials in the mentioned table being just up to 2. For rings that are not prime powers, the sizes of this gap seem (for small values of \( n \)) quite unintuitive, which suggests that the formula governing that size is complicated. For larger values of \( n \), and for all rings, the gap sizes seem to build on previous values, via multiplication by the ring size. Arguably, the general formula for the last gap size may be simplest when the degree of the polynomials is completely unbounded.

In Chapter 5 we presented many concrete metrics of solution spaces for small rings and small polynomials (due to computational limitations). From them we were able to notice certain properties, that may also be true in general cases. Some of them may be relatively easy to prove, or are just quite interesting. We list three most intriguing ones, as following hypotheses:

1. Polynomials of \( n \) variables, of degree up to 2, over finite fields of prime size \( p \), can only have one of \( 2\left\lfloor \frac{n}{2} \right\rfloor + 3 \) numbers of solutions if \( p = 2 \), and one of \( 4(\left\lfloor \frac{n}{2} \right\rfloor + 1) \) when \( p \geq 3 \).

2. Numbers of possible numbers of solutions of polynomials over rings \( \mathbb{Z}_m \), of \( n \) variables and degree up to \( d \), can be bounded by a polynomial in \( r, n \) and \( d \). This is especially plausible when \( m \) is prime or a prime power and \( d \) is small.

3. If \( m = p_1^{i_1}p_2^{i_2} \ldots p_k^{i_k} \), then the number of possible solution numbers of polynomials of \( n \) variables, of degree up to \( d \) over \( \mathbb{Z}_m \), is a function of the numbers of possible solution numbers of polynomials of the same number of variables and degree, over each of \( \mathbb{Z}_{p_i^{i_k}} \), \( i < k \). For an example, see \( r = 2, 3, 6 \) and \( n = 2, 3 \) in Table 9.

There are some more, potentially general, properties that we described in Chapter 5, and certainly many more than we did not notice, or that require more experimental results to become noticeable. Yet, it certainly seems that this area is very rich in interesting, open mathematical problems, which additionally, due to increasing understanding of polynomials behaviour over rings, have a potential to be useful to complexity theory.

Despite the pathology of zero-divisors, we believe that the solution sets of polynomials modulo composites should have a natural, attractive, and unifying theory. Such work would seem relevant to the
prospects for progress in complexity lower bounds. We hope that this research promotes interest and strategies in expanding this theory.

Acknowledgments

We would like to thank Pete L. Clark for bringing [21] to our attention, which led us to [23], and for further comments on this draft. We also thank him and Hui June Zhu and Todd Cochrane for consultation on the state of mathematical knowledge in the domain of this paper.

References

[1] S. Aaronson and D. Gottesman. Improved simulation of stabilizer circuits. *Phys. Rev. A*, 70(052328), 2004.

[2] L. Adleman, J. DeMarrais, and M.-D. Huang. Quantum computability. *SIAM J. Computing*, 26(5):1524–1540, 1997. SICOMP:10.1137/S0097539795293639.

[3] Alan Adolphson and Steven Sperber. $p$-adic estimates for exponential sums and the theorem of Chevalley-Warning. In *Annales scientifiques de l’École Normale Supérieure*, volume 20(4), pages 545–556. Société mathématique de France, 1987.

[4] James Ax. Zeros of polynomials over finite fields. *American Journal of Mathematics*, 86(2):255–261, 1964.

[5] D. Bacon, W. van Dam, and A. Russell. Analyzing algebraic quantum circuits using exponential sums. http://www.cs.ucsb.edu/~vandam/LeastAction.pdf, November 2008.

[6] David Brink. Chevalleys theorem with restricted variables. *Combinatorica*, 31(1):127–130, 2011.

[7] Jin-Yi Cai, Xi Chen, and Pinyan Lu. Graph homomorphisms with complex values: A dichotomy theorem. *SIAM Journal on Computing*, 42(3):924–1029, 2013.

[8] Wei Cao. Dilation of Newton polytope and $p$-adic estimate. *Discrete and Computational Geometry*, 45(3):522–528, 2011.

[9] Wei Cao. A partial improvement of the Ax–Katz theorem. *Journal of Number Theory*, 132(4):485–494, 2012.

[10] Wei Cao and Qi Sun. A reduction for counting the number of zeros of general diagonal equation over finite fields. *Finite Fields and Their Applications*, 12(4):681–692, 2006.

[11] Wei Cao and Qi Sun. Improvements upon the Chevalley–Warning–Ax–Katz-type estimates. *Journal of Number Theory*, 122(1):135–141, 2007.

[12] Francais. Castro and Francais N. Castro-Velez. Improvement to Moreno-Moreno’s theorems. *Finite Fields and Their Applications*, 18(6):1207–1216, 2012.

[13] Claude Chevalley. Démonstration d’une hypothèse de M. Artin. *Abhandlungen aus dem Mathematischen Seminar der Universität Hamburg*, 11(1):73–75, 1935.

[14] Pete L Clark, Aden Forrow, and Schmitt John R. Warning’s second theorem with restricted variables. 2014. http://www.math.uga.edu/~pete/Clark-Forrow-Schmitt14.pdf.

[15] Christopher M Dawson, Henry L Haselgrove, Andrew P Hines, Duncan Mortimer, Michael A Nielsen, and Tobias J Osborne. Quantum computing and polynomial equations over the finite field $Z_2$. *arXiv preprint quant-ph/0408129*, 2004.
[16] Bernard Dwork. On the rationality of the zeta function of an algebraic variety. *American Journal of Mathematics*, 82(3):631–648, 1960.

[17] Lance Fortnow and John Rogers. Complexity limitations on quantum computation. In *Computational Complexity, 1998. Proceedings. Thirteenth Annual IEEE Conference on*, pages 202–209. IEEE, 1998.

[18] D. Gottesman. The Heisenberg representation of quantum computers. [http://arxiv.org/abs/quant-ph/9807006](http://arxiv.org/abs/quant-ph/9807006), 1998.

[19] D Roger Heath-Brown. A note on the Chevalley-Warning theorems. *Russian Mathematical Surveys*, 66(2):427, 2011.

[20] Xiang-Dong Hou. A note on the proof of a theorem of Katz. *Finite Fields and Their Applications*, 11(2):316–319, 2005.

[21] Daniel J Katz. Point count divisibility for algebraic sets over $\mathbb{Z}/p^r\mathbb{Z}$ and other finite principal rings. *Proceedings of the American Mathematical Society*, 137(12):4065–4076, 2009.

[22] Nicholas M Katz. On a theorem of Ax. *American Journal of Mathematics*, 93(2):485–499, 1971.

[23] Murray Marshall and Garry Ramage. Zeros of polynomials over finite principal ideal rings. *Proceedings of the American Mathematical Society*, 49(1):35–38, 1975.

[24] Oscar Moreno and C.J. Moreno. Improvements of the Chevalley-Warning and the Ax-Katz theorems. *American Journal of Mathematics*, 117(1):241–244, 1995.

[25] Oscar Moreno, Kenneth W Shum, Francis N Castro, and P Vijay Kumar. Tight bounds for Chevalley–Warning–Ax–Katz type estimates, with improved applications. *Proceedings of the London Mathematical Society*, 88(3):545–564, 2004.

[26] Kenneth Regan and Amlan Chakrabarti. Quantum circuits, polynomials, and entanglement measures, 2012. Working Draft, [http://www.cse.buffalo.edu/~regan/papers/pdf/ReCh12.pdf](http://www.cse.buffalo.edu/~regan/papers/pdf/ReCh12.pdf).

[27] Stephen H Schanuel. An extension of chevalley’s theorem to congruences modulo prime powers. *Journal of Number Theory*, 6(4):284–290, 1974.

[28] Daqing Wan. An elementary proof of a theorem of Katz. *American Journal of Mathematics*, 111(1):1–8, 1989.

[29] Daqing Wan. A Chevalley-Warning approach to $p$-adic estimates of character sums. *Proceedings of the American Mathematical Society*, pages 45–54, 1995.

[30] Ewald Warning. Bemerkung zur vorstehenden Arbeit von Herrn Chevalley. *Abh. Math. Sem. Univ. Hamburg*, 11:76–83, 1936.

[31] Ryan Williams. Non-uniform ACC circuit lower bounds. In *Computational Complexity (CCC), 2011 IEEE 26th Annual Conference on*, pages 115–125. IEEE, 2011.

[32] Richard M Wilson. A lemma on polynomials modulo $p^m$ and applications to coding theory. *Discrete mathematics*, 306(23):3154–3165, 2006.