Simultaneous Solutions to Diagonal Equations over the p-adic Numbers and Finite Fields, and some Connections with Combinatorics

by

Ivan Daniel Meir

Submitted for the degree of

PhD

Department of Pure Mathematics

January 1997

Accepted 1997

Summary

Ivan D Meir

Simultaneous Solutions to Diagonal Equations over the p-adic Numbers and Finite Fields, and some Connections with Combinatorics

The first part of this thesis is devoted to solving simultaneous diagonal equations over the p-adic numbers. It is known that a system of r additive equations of degree k with greater than $2rk$ variables has a non-trivial p -adic solution for all $p > k^{2r+2}$. In particular, for two diagonal equations with greater than $4k$ variables we have a non-trivial p-adic solution for all $p > k^6$. In part II we improve this to $p > 3k^4$. A considerable modification of the standard method of exponential sums is introduced which uses the Hasse-Weil sum estimate for multiplicative characters. We also consider the same system with more than crk variables, $c > 2$, and show the existence of a non-trivial solution for all $p > r^2k^{2+\frac{2}{c-2}}$ if $r \neq 1$, and $p > k^{2+\frac{2}{c-1}}$ if $r = 1$. In Chapter 3 we conjecture a generalisation of the Hasse-Weil estimate to polynomials in greater than two variables and discuss the possibility of applying this to r diagonal equations, where $r > 2$.

In part III, we first establish a new and unexpected connection between equations over finite fields and Ramsey theory, by relating the problem of finding monochromatic triangles to finding a solution of two diagonal equations with exactly three variables non-zero. This is also generalised to hypergraphs with monochromatic r-sets. We then look at the Paley graph (or quadratic residue graph) and consider various related graphs, including a new hypergraph generalisation. We then use the conjectured generalisation of the Hasse-Weil estimate to improve a result of Bollobás on subgraphs contained within the Paley graph, which is applied to give new results concerning quadratic residue difference sets.

Acknowledgements

I would like to thank Sheffield University for providing funding for the three years of my PhD. I also extend my thanks to Professor R. J. Cook for suggesting this area of research and giving much helpful advice and support over the last four years.

I would also like to thank my parents, my twin brother Adam and Clare for helping me and supporting me in many very important ways throughout my studies.

Contents

[1]**The contents of this chapter have been accepted for publication in the Journal of Number Theory.**

Part I

Survey and Methods

Chapter 1

Survey

1.1 Introduction

Parts 1 & 2 of this thesis are devoted to looking at solutions of equations over the p-adic numbers and finite fields; however I begin with a brief survey of the theory of equations over the integers and rationals also. This is done for completeness, and also as a partial motivation for our original question. For this survey I have drawn extensively from articles by Le Veque and Lewis in the excellent volume 6 of the MAA Studies in Mathematics series [42].

(For reasons beyond the author's control, to show that two integers are not congruent it has been necessary to use the symbol '$\not=$' instead of 'not-equivalent to'.)

1.2 Diophantine equations

Any equation in one or more unknowns is called a diophantine equation if one asks for solutions in integers or sometimes rationals.

The study of diophantine equations, and its name, goes back to the Greek mathematician Diophantus of Alexandria (c. 250 A.D.) whose work involved the solution of many problems involving integer or rational numbers. He did not develop a general or systematic approach to the subject but showed that here was an area worthy of study. Diophantus' work, through a second translation by C. Bachet, was much studied by Pierre de Fermat. He showed that the equation $x^4 + y^4 = z^4$ has no solution in non-zero integers, solved completely the problem of

representing integers as the sum of two squares, and he claimed without publication a proof that every integer is the sum of four squares. He was also the originator of the famous Fermat's last theorem; the equation $x^n + y^n = z^n$ has no solution x, y, z with $xyz \neq 0$ for $n \geq 3$. This has recently been proved by the Princeton mathematician Andrew Wiles, using the theory of elliptic equations and modular forms.

Following Fermat, mathematicians such as Euler, Lagrange, Gauss and Kummer all made further contributions to the the subject. Although their work was mainly limited to quadratic equations, such as the Pell equation, $x^2 - dy^2 = c$, or to equations of special form, such as Fermat's equation, much of modern number theory has flowed from their investigations. Implicit in the work of Gauss, for example, are many indications of modern developments such as elliptic curves and the Riemann hypothesis over finite fields. Also the difficulties encountered by Kummer in studying Fermat's equation, led to far-reaching developments in algebra and the theory of algebraic numbers which are now potent tools for attacking other diophantine problems.

1.2.1 Binary equations

A binary equation is an equation of the form $f(x, y) = 0$, where f is a polynomial in two variables. In geometrical terms such an equation $f(x, y) = 0$ is represented by a certain curve, if x and y take real values, or by a Riemann surface, if x and y may take complex values. An important concept in algebraic geometry is birational transformation. For curves these transformations take the form

$$\begin{aligned} x &= \phi(z, u), \\ y &= \psi(z, u), \end{aligned}$$

where ϕ and ψ are rational functions of z and u, and when $f(x, y) = 0$, z and u are also rational functions of x and y,

$$\begin{aligned} z &= \Phi(x, y), \\ u &= \Psi(x, y). \end{aligned}$$

There is a 1-1 correspondence between points on the transformed curves which means that information about the new curve should have implications for the old. The form and degree of the equations may change, but there is a number called the genus of the curve, a non-negative integer, which remains unchanged under birational transformations. (It is the topological genus of the Riemann surface of f.) Mathematicians have found that classifying curves by genus also classifies them very well according to their diophantine properties. Curves of genus 0 are especially simple: If $f(x,y) = 0$ is of genus 0, then it is parametrizable by rational functions of a variable t, that is, $f(x,y) = 0$ can be written in parametric form as $x = g(t)$, $y = h(t)$, with g and h rational. For example, $x^2 + y^2 = 1$ has rational parametrization $x = \dfrac{2t}{1+t^2}$, $y = \dfrac{1-t^2}{1+t^2}$.

Unfortunately, because g and h may have non-rational coefficients, this does not directly give us integer or rational solutions. Hilbert and Hurwitz [39] used the parametrizability of curves of genus 0 to relate rational points on curves of genus 0 to first and second degree curves. In modern terminology we have the following statements:

1. *A curve of genus 0 defined over $\mathbb{Q}$ is birationally equivalent over $\mathbb{Q}$ either to the line or to the conic.*

2. *A conic defined over $\mathbb{Q}$ is birationally equivalent to the line if and only if it has a rational point.*

Hence the theory of rational solutions is reduced to deciding when a conic defined over $\mathbb{Q}$ has a rational point. In fact, conditions for the existence of a rational point on a conic had been given by Legendre. It was reformulated by Hasse using the field of p-adic numbers, $\mathbb{Q}_p$, into the following result which anticipates our later discussion of the Hasse Principle:

A necessary and sufficient condition for the existence of a rational point on a conic C defined over $\mathbb{Q}$ is that there is a point on C defined over the real field $\mathbb{R}$ and over $\mathbb{Q}_p$ for every prime p.

The question of solutions in integers remained open until the later work of Thue. He [60] concerned himself with diophantine equations of the form

$$a_0x^n + a_1x^{n-1}y + \cdots + a_ny^n = m, \qquad a_0 \neq 0.$$

This can be written in the form

$$a_0(x-\alpha_1 y)\cdots(x-\alpha_n y)=m,$$

where $\alpha_1,\ldots,\alpha_n$ signify a complete set of conjugate algebraic numbers. Thus, if the equation is soluble in positive integers x,y, then the nearest of the numbers $\alpha_1,\ldots,\alpha_n$ to x/y, say α, satisfies

$$|x-\alpha y|\ll 1,$$

where $a\ll b$ means $a<bc$ for some positive constant c. Now for y sufficiently large and $\alpha\neq\alpha_j$, we have

$$|x-\alpha_j y|=|(x-\alpha y)+(\alpha-\alpha_j)y|\gg y,$$

giving

$$|x-\alpha y|\ll\prod_{\alpha_j\neq\alpha}|x-\alpha_j y|^{-1}\ll 1/y^{n-1}\Longrightarrow|\alpha-x/y|\ll 1/y^n. \tag{1.1}$$

Thue then reasoned that one might be able to show that (1.1) cannot have infinitely many integer solutions—this is a problem of diophantine approximation. This Thue achieved using a very complicated argument.

Curves of genus 0 and 1 were investigated by Poincaré. He analysed the conditions for a curve of genus 0 to have finitely or infinitely many rational points. He also considered the very important class of elliptic curves, curves of genus 1 with a rational point, and showed that they are birationally equivalent over $\mathbb{Q}$ to the form

$$y^2=4x^3+ax+b. \tag{1.2}$$

However, even today the rational solutions of (1.2) are still not decided.

Poincaré's investigations also included the following far-reaching and ambitious theory. Although only curves of genus 0 have rational parametrization, by replacing rational functions by transcendental functions we can give a similar representation for curves of positive genus, considering a set of g points if the curve is of genus g. The 'coordinates' of the set are those parameters which yield a certain set of g points, and it turns out that if two such sets are

rational, in a certain sense, then we can produce a third rational set by termwise addition of the coordinates; one calls the third set the sum of the other two. In the case of the elliptic curves this is the classical 'chord and tangent process'—if P and Q are two rational points, then the line joining P and Q intersects the curve in another rational point.

The next major development came when L. Mordell attempted to prove that a certain equation of genus 1 has only finitely many solutions. His final result was very different from his initial intentions. Poincaré had shown how to add two points p_1, p_2 on a curve of genus 1 to obtain a third point. In this way we can get $sp_1 + tp_2$, where s, t are any integers. More generally we can start with n rational points $p_1, \ldots, p_n$ and obtain the further rational points $s_1p_1 + \cdots + s_np_n$. It could be possible that no matter how one chooses the points $p_1, \ldots, p_n$ there are rational points which are not obtained in this manner. What Mordell showed [48] was, if the curve had a cubic or quartic equation with integral coefficients and was of genus 1, then there is invariably a finite collection of rational points on the curve such that every rational point can be expressed as a linear combination of them. In group-theoretic terms we say that the group of points is finitely-generated. This had been conjectured but not proved by Poincaré.

A. Weil [63] vastly extended Mordell's theorem by showing that it holds for arbitrary curves of genus 1 whose equations have algebraic coefficients, and for points with coordinates in a fixed algebraic number field. He also obtained the analogous result for curves of higher genus, in which 'rational point' is replaced by 'rational set of g points'.

In 1921 C. Siegel strengthened Thue's results on (1.1), proving the Thue-Siegel theorem, and made a number of new applications to diophantine equations. In 1929 he published a major work [56] combining his refinement of Thue's inequality together with the Mordell-Weil theorem. Siegel showed that no curve of positive genus has infinitely many integer points on it, and with the Hilbert-Hurwitz-Poincaré analysis he gave an explicit characterisation of those curves of genus 0 with infinitely many integer points.

An important recent result in this area has been Falting's proof of the Mordell conjecture that there are only finitely many rational points on a curve of genus greater than 1. This shows that Fermat's equation has only finitely many solutions for each n.

1.2.2 p-adic methods

It is in the study of curves of genus 1 that we see the introduction of p-adic methods. One powerful method of testing whether an equation has rational solutions is to ask whether it has solutions in some larger field containing the field of rational numbers. For example the equation $x^2 + y^2 = -1$ has no rational solutions because it has no real solutions. Besides the real field we have others, such as the p-adic field (which contains the rational field), in which it is sometimes quite easy to show that an equation has no solution. We remark that an equation $f(x_1, \ldots, x_n) = 0$ has a p-adic solution, where p is prime, if and only if, for each positive integer N, there are integers $a_1(N), a_2(N), \ldots, a_n(N)$, not all divisible by p such that $f(a_1(N), \ldots, a_n(N))$ is divisible by p^N. Since 0 is divisible by every integer, the existence of a p-adic solution (for every p) is necessary if the equation is to have a solution in integers, as is the existence of real solutions. We have seen this earlier in Hasse's version of the local-global principle for conics.

The main motivation however, for studying p-adic solutions is the possibility of this working the other way around: if there are real solutions and p-adic solutions for every p, then the equation has a solution in integers; when this is the case, we say that the Hasse principle applies. This is known to be true, for example, for all quadratic equations and for all curves of genus 0, but it is not always valid. H. Reichardt (1942) and Lind (independently) gave the example of the curve $x^4 - 17 = 2y^2$ of genus 1 , which has p-adic solutions for all p, and real solutions, but no solutions in integers. Many more examples have subsequently been given.

Even if a Hasse principle holds, it would seem to replace the problem by having to demonstrate p-adic solvability for each of infinitely many primes. Fortunately, by Theorem 3 below of Lang-Weil, p-adic solvability is automatic for all sufficently large primes. For each prime, solvability can be decided one way or another in a finite number of steps, so that in theory the Hasse principle is completely effective when it applies.

1.2.3 Fermat's method of descent

If a finite number of rational points on the curve are known, then the p-adic method is usually of no use in showing that there are no others. In this case we can sometimes use a device invented by Fermat, the 'method of infinite descent'. The method involves finding a birational

transformation τ of the curve into itself such that every rational point p on the curve is of the form $\tau(q)$, where q is another rational point. Then one finds a way of associating with each rational point p a certain positive integer $H(p)$ which in some way measures the 'complexity' of the point, and is such that if $p = \tau(q)$ is different from any of the rational points already known, then $H(q) < H(p)$. Then if there were additional solutions, there would be one for which $H(p)$ is smallest—but this is impossible, since $H(q)$ is even smaller. Fermat originally applied this technique to prove that there are no integer solutions of

$$X^4 + Y^4 = Z^4 \qquad X \neq 0, Y \neq 0.$$

He remarked that it is enough to disprove

$$X^4 + Y^4 = Z^2 \qquad X \neq 0, Y \neq 0$$

which is an elliptic curve, although not in canonical form.

This can also be applied to curves of arbitrary genus, but here there is a problem of finding a suitable transformation. This is easy for curves of genus 1, and the method can be pushed much further. There is much current research done in this direction.

1.3 Equations in Many Variables

For equations with more than 2 variables, no general method or approach, similar to the ones we have just seen for curves, is known. It is is this area, however, that the developments most related to this thesis have occurred, therefore it is here that we shall concentrate. The starting point is along somewhat different lines than before: one considers a whole family of equations of similar form, but having different numbers of variables, and asks whether those having sufficiently many variables must always be solvable, and if so, how many variables are necessary. This approach is exemplified by the conjecture of E. Waring [62] (1770) that for each exponent k, the equation

$$x_1^k + x_2^k + \cdots + x_s^k = n, \qquad x_1 > 0, \ldots, x_s > 0 \tag{1.3}$$

is solvable, for each positive integer n, if s is sufficiently large.

This was proved by Hilbert in 1909. If $g(k)$ is the smallest value of s for which (1.3) is solvable for every positive n, then the determination of $g(k)$ is now nearly complete. The exact value can be computed for each $k \geq 5$, and for all but finitely many positive integers k, $g(k) = 2^k + A - 2$, where A is the largest integer not exceeding $(\frac{3}{2})^n$; see Vaughan [61].

Now let $G(k)$ denote the smallest value of s for which (1.3) is solvable for every sufficiently large n. The function $G(k)$ is more natural for this problem since it excludes the possibility of a few small integers n requiring abnormally many kth powers, thereby artificially increasing the size of $g(k)$. Questions concerning $G(k)$ are much more difficult, and few exact values for $G(k)$ are known.

G. H. Hardy and J. E. Littlewood conjectured that $G(k) < 2k + 1$ when k is not a power of 2, and that $G(k) < 4k$ when it is. It is here that Hardy and Littlewood introduced their famous 'circle method'. Their technique was to develop an approximate formula for the number of solutions of (1.3) and to deduce that this was positive for s sufficiently large.

There are two components in the principal term of the approximate formula, one factor (the singular integral) corresponding to the real solutions of (1.3), and the other (the 'singular series') to the number of p-adic solutions for the various primes p. Since the approximate formula consists of the principal term plus an error term, it is necessary to verify that the p-adic solution factor, which is independent of n, is different from 0; this is possible exactly when n is greater than the upper bound for $G(k)$ conjectured by Hardy and Littlewood. The still larger bound for s is necessary to prove that the error term is of smaller order of magnitude than the principal term.

Similar methods can be used for many variations on Waring's problem. The first part of this thesis is devoted to studying one of these over the p-adic numbers:

$$f_i(\mathbf{x}) = a_{1i}x_1^k + \cdots + a_{ni}x_n^k = d_i, \qquad 1 \leq i \leq r \tag{1.4}$$

In fact in order to find integer solutions to (1.4) we must first obtain p-adic solutions and then use the Hardy-Littlewood method to give us solutions in integers.

For example, Davenport and Lewis [23] (1963) proved the following result: Let $c_1, \ldots, c_s$

be non zero integers, not all of the same sign if k is even, and suppose that $s > k^2$. Then the equation $c_1x_1^k + \cdots + c_sx_s^k = 0$ has infinitely many solutions in non-zero integers $x_1, \ldots, x_s$. In this case, in contrast to Waring's problem, it is the p-adic component of the question which provides the lower bound on s, rather than the associated formula for the number of real solutions.

A set of values of the variables for which a certain polynomial vanishes is called a zero of the polynomial, and since clearly $f(0,0,\ldots,0) = 0$ if $f(x_1,\ldots,x_n)$ has no constant term, it is customary to refer to $(0,0,\ldots,0)$ as the *trivial zero* of a form.

A. Meyer proved in 1884 that every quadratic form with integer coefficients assumes the value 0 for integer values of the variables $x_1,\ldots,x_n$, not all zero, if $n > 5$ and the form vanishes for real values of the variables, not all zero.

It was generally felt that a form of fixed degree, or a system of forms of fixed degrees, should have an integer zero if they have a real zero, for sufficiently many variables. E. Artin pointed out in the 1930s that, for each degree d, there are 'norm forms' in d^2 variables which have only the trivial zero; these are forms like $x^2 - 2y^2 = (x - \sqrt{2}y)(x + \sqrt{2}y)$ which split into linear factors with irrational coefficients, and whose vanishing at a non-trivial point would be impossible (i.e if $x^2 - 2y^2 = 0$ then $\frac{x}{y} = \pm\sqrt{2}$, which is false since $\sqrt{2}$ is irrational). It follows that for every set of degrees $d_1,\ldots,d_r$, there are forms $f_1,\ldots,f_r$ having those degrees and not having a common non-trivial zero, if there are at most $d_1^2 + d_2^2 + \cdots + d_r^2$ variables. Artin conjectured that this number of variables, plus 1, is sufficient to guarantee the existence of a non-trivial zero, in integers or in p-adic numbers, so long as the system has a non-trivial real zero. Meyer's theorem is exactly the case $r = 1$, $d = 2$, and the p-adic conjecture was proved for a single cubic form by Lewis [43] and for two quadratics by V. Demyanov [29]. For simultaneous quadratic forms see Birch, Lewis and Murphy [9].

In 1944 R. Brauer proved a qualitative form of the p-adic Artin conjecture, namely that a system of forms of fixed degrees has a p-adic zero provided the number of variables is sufficiently large. R.Brauer [14] was the first to obtain a general result for integer solutions of forms of high degree. B. Birch [8] modified and extended Brauer's result to show that an arbitrary system of forms of odd degree with sufficiently many variables has a zero in integers. The Brauer-Birch method needs a large number of variables to imply a rational zero: they need over 500 variables

to infer that a cubic form has a rational zero. Thus it is natural to seek methods which require fewer variables. It should be noted however that the existence of such a bound is a special property of forms of odd degree. The form

$$\left(\sum_{v=1}^{N} x_v^2\right)^2 - 3\left(\sum_{v=1}^{N} y_v^2\right)^2$$

has no rational zero regardless of the size of N although it is indefinite and has p-adic zeros, for every p, when $N \geq 5$.

In his paper, Brauer proved that there exists a function $\varphi_p(d)$ such that every form of degree d in $m \geq \varphi_p(d)$ variables with coefficients in a p-adic field has a zero in that field. It was conjectured by Artin that one could take $\varphi_p(d) = d^2 + 1$. This is the case for $d \leq 3$, but the conjecture is false for infinitely many d.

By means of ultraproducts and some sophisticated extensions of valuation theory, Ax and Kochen [6] have proved that if $n > d_1^2 + \cdots + d_r^2$, a system of forms in n variables with p-adic coefficients has a p-adic zero for all sufficiently large $p > p_0$. Unfortunately their proof is ineffective. However, our Theorem 26 in Chapter 5 shows that for the case of diagonal equations we have $p_0 \leq r^2 k^{2+\frac{2}{k-2}}$, $r \neq 1$, $k > 2$.

The first counter-example to Artin's conjecture was given by Terjanian [58]. He observed that

$$\begin{aligned} G(\mathbf{x}) &= G(x_1, x_2, x_3) \\ &= x_1^4 + x_2^4 + x_3^4 - x_1^2x_2^2 - x_1^2x_3^2 - x_2^2x_3^2 - (x_1x_2x_3)(x_1 + x_2 + x_3) \end{aligned}$$

is such that $G(\mathbf{x}) \equiv \begin{cases} 1 \pmod 4, & \text{if some } x_i \text{ is odd} \\ 0 \pmod{16}, & \text{if all } x_i \text{ are even.} \end{cases}$

Hence

$$F = G(\mathbf{x}) + G(\mathbf{y}) + G(\mathbf{z}) + 4G(\mathbf{u}) + 4G(\mathbf{v}) + 4G(\mathbf{w})$$

is a form in $18 > (4^2+1)$ variables which has only the trivial solution in $\mathbb{Q}_2$.

Browkin [15] has shown the existence of a function $\lambda(p)$ s.t. $\lim_{p\to\infty} \lambda(p) = 0$ and the existence of forms G_p over $\mathbb{Z}$ of degree d in $n > d^{3-\lambda(p)}$ variables having only the trivial solution

in $\mathbb{Q}_p$.

1.3.1 Equations over the p-adics and finite fields

Artin's conjecture for p-adic numbers is an example of one extreme in the theory; take a large number of variables and look to prove p-adic solubility for all p. The other is to take a smaller, fixed number of variables and to find a bound P such that the equations have a p-adic solution for all $p > P$. This is the problem that we consider in part II of this thesis. Now a prerequisite to finding p-adic solutions is to find solutions (mod p). We also have the following theorem derived from the methods of Hensel and Newton. The statement and proof have been taken from the article by D. J. Lewis in [42].

Theorem 1 *Let $f_1, \ldots, f_r$ be polynomials with integer coefficients. If $a_1, \ldots, a_m$ are integers such that $f_v(a_1, \ldots, a_m) \equiv 0 \pmod{p}$, $v = 1, \ldots, r$ and the vectors $(u_{11}, \ldots, u_{1m}), \ldots, (u_{r1}, \ldots, u_{rm})$, where $u_{ij} = (\partial f_i/\partial x_j)(a_1, \ldots, a_m)$, are linearly independent modulo p, then for each $T \geq 1$ the set of congruences $\left\{f_v \equiv 0 \pmod{p^T}\right\}$ has a solution $a_{1T}, \ldots, a_{mT}$, where $a_j \equiv a_{jT} \pmod{p}$, $j = 1, \ldots, m$.*

Proof. The proof is by induction on T. By hypothesis the result is true for $T = 1$. Suppose the result is true for $T \leq N$; then

$$f_v(a_{1N}, \ldots, a_{mN}) = p^N b_{vN}$$

and

$$\partial f_i/\partial x_j(a_{1N}, \ldots, a_{mN}) \equiv u_{ij} \pmod{p}.$$

Put $a_{jN+1} = a_{jN} + p^N y_i$, $j = 1, \ldots, m$. Then

$$\begin{aligned} f_v(a_{1N+1}, \ldots, a_{mN+1}) &\equiv f_v(a_{1N}, \ldots, a_{mN}) + p^N \sum_{j=1}^{m} u_{vj} y_j \pmod{p^{N+1}} \\ &\equiv p^N (b_{vN} + \sum_{j=1}^{m} u_{vj} y_j) \pmod{p^{N+1}}. \end{aligned}$$

Since the matrix (u_{ij}) has rank r (mod p), the set of linear congruences $b_{vN} + \sum_{j=1}^{m} u_{vj} y_j \equiv 0$ (mod p) is soluble, and consequently we have the desired result for $T = N + 1$. ■

Thus, given a mod p solution that is non-singular in some sense, we can generate non-trivial p-adic solutions.

Thus we have swapped looking for zeros in $\mathbb{Z}/p^n$, a ring with divisors of zero, with the field $\mathbb{Z}/p$. Also, as C. Chevalley [17] has shown, finite fields are nearly algebraically closed. Chevalley's theorem states:

Theorem 2 *Every homogeneous polynomial over a finite field $\mathbb{F}$ of degree d in $m > d$ variables has a zero in $\mathbb{F}$.*

Questions concerning zeros in $\mathbb{Z}/p$ can be approached by means of exponential sums, the method we shall introduce in Chapter 3. This method is indispensible for the results proved in this thesis.

The theory of equations over finite fields is a very difficult and technical area, the main result being the Riemann hypothesis for varieties over finite fields, conjectured by Weil [64] and proved by Pierre Deligne [28] in 1974. We shall discuss some of these developments in Chapter 3.

For equations $f(x_1, \ldots, x_n) = 0$ and systems of such equations, the first general result of importance was that of Lang and Weil [41], which can be conveniently stated in terms of projective varieties, (in simple terms the solution space of a set of homogeneous polynomials). Here, $\mathbb{F}_q$ is the finite field of q elements where $q = p^r$ for some prime p.

Theorem 3 *If V is an absolutely irreducible variety in the n-dimensional projective space over $\mathbb{F}_q$ and V is of dimension r and degree d, then the number N_1 of $\mathbb{F}_q$-rational points of V satisfies*

$$|N_1 - q^r| \leq (d-1)(d-2)q^{r-\frac{1}{2}} + A(n,r,d)q^{r-1}.$$

Here, *absolutely irreducible* means that the variety cannot be decomposed into further varieties. *Projective space* is just affine space together with points at infinity, basically the set of 1-dimensional subspaces of $\mathbb{F}_q^{n+1}$.

The form of this estimate is typical. In order to give a lower bound for q, we take the difference between the number of solutions and the 'average' number of solutions, and show that this is $o(q^r)$. This theorem was proved using the Riemann hypothesis over finite fields for

curves, but for diagonal varieties, as we show in chapter 5 a similar theorem can be proved using elementary methods. As we shall see in chapter 3 the Riemann hypothesis over finite fields is also related to multiplicative character sum estimates. We now look at diagonal equations over the finite fields and review some results.

1.3.2 Diagonal equations

Let us consider a set of r additive equations

$$f_i(\mathbf{x}) = a_{1i}x_1^k + \cdots + a_{ni}x_n^k = 0, \qquad 1 \leq i \leq r \tag{1.5}$$

with coefficients in $\mathbb{Z}$. First we look at a number of examples which help us to see what is possible in this area.

We note that the condition $p \equiv 1 \pmod{k}$ is important since otherwise all residues are kth powers mod p and (1.5) reduces to a set of linear equations which can easily be solved.

Example 4 *Let p be any prime with $p \equiv 1 \pmod{k}$, and let δ be a kth power non-residue. Then the equation*

$$\sum_{i=1}^{k} p^{i-1}(x_i^k - \delta y_i^k) = 0 \tag{1.6}$$

in $n = 2k$ variables has no non-trivial solution in p-adic integers.

Proof. If (1.6) has a solution in p-adic integers then there exists a smallest integer $N > 0$ such that p^N is the highest power of p dividing $\sum_{i=1}^{k} p^{i-1}(x_i^k - \delta y_i^k)$ with x_i, y_i not all divisible by p. Then this implies that $x_1^k - \delta y_1^k$ is divisible by p, an impossibility unless $x_1 \equiv y_1 \equiv 0$ mod p, since δ is a k-th power non-residue. If $x_1 \equiv y_1 \equiv 0$ mod p then there must exist another pair x_j, y_j not both not divisible by p. Substitute $x_1 = px_1'$ and $y_1 = py_1'$ into (1.6) and divide through by p. We then have another set of x_i, y_i not all divisible by p such that p^{N-1} is the highest power dividing $\sum_{i=1}^{k} p^{i-1}(x_i^k - \delta y_i^k)$, contrary to our initial assumption regarding N. ■

Thus if we take r disjoint copies of (1.6) this gives us r equations in $2rk$ variables which have no non-trivial solution in p-adic integers, for infinitely many primes p. This shows that in order to get a bound for p we must take $n > 2rk$.

Example 5 *Let k be an exponent such that $k = p - 1$ for some prime p. Then the equation*

$$\sum_{i=1}^{k} p^{i-1} \sum_{j=1}^{k} x_{ij}^{k} = 0 \tag{1.7}$$

in k^2 variables has no non-trivial p-adic solution.

Proof. $x^k \equiv x^{p-1} \equiv 0$ or $1 \pmod{p}$ so $\sum_{j=1}^{k} x_{ij}^{k} \equiv 0 \pmod{p}$ implies $x_{ij} \equiv 0 \pmod{p}$ for $1 \leq j \leq k$. This being shown, the proof proceeds as above. ■

As before, r disjoint copies of (1.7) gives us r equations in rk^2 variables which have no non-trivial p-adic solution. Thus, any bound on the number of variables which gives a solution for all p, must be at least $n > rk^2$. Let us now look at some more specific results.

1.3.3 One additive equation, $r = 1$

If $k = 2$, we have p-adic solvability for every prime p provided $n \geq 5 = 2.2 + 1$. This is best possible using example 4. For $k = 3$, Lewis [44] showed that we have a non-trivial solution if $n \geq 7 = 2.3 + 1$. This is again best possible from example 4. In the case $k = 5$, Gray [37] showed that we have a solution in every p-adic field provided $n \geq 16 = 3.5 + 1$. This is best possible as

$$\sum_{i=1}^{5} 11^{i-1}(x_i^5 + 2y_i^5 + 4z_i^5) = 0 \tag{1.8}$$

has no non-trivial solution in 11-adic integers.

Davenport and Lewis [23] showed that for any $k > 1$ the equation (1.5) has a non-trivial solution in p-adic integers provided that $n \geq k^2 + 1$.

1.3.4 Two additive equations, $r = 2$

For $k = 2$, two quadratic equations (not necessarily additive) have a non-trivial solution in p-adic integers for all primes p provided $n \geq 9$ (see Demanyov [29]), and this is best possible.

When $k = 3$, Davenport and Lewis [24] showed that two additive equations have a non trivial solution in p-adic integers for every prime p provided that $n \geq 16$. Also they gave the

example

$$\begin{aligned}\phi(x_1,\ldots,x_5)+7\phi(y_1,\ldots,y_5)+49\phi(z_1,\ldots,z_5) &= 0,\\ \psi(x_1,\ldots,x_5)+7\psi(y_1,\ldots,y_5)+49\psi(z_1,\ldots,z_5) &= 0,\end{aligned}$$

where

$$\begin{aligned}\phi(x_1,\ldots,x_5) &= x_1^3+2x_2^3+6x_3^3-4x_4^3,\\ \psi(x_1,\ldots,x_5) &= x_2^3+2x_3^3+4x_4^3+x_5^3,\end{aligned} \tag{1.9}$$

which has no solution in the 7-adic field. Cook [19] however has shown that for all $p \neq 7$, we have a p-adic solution for $n \geq 13$. This is best possible in view of example 4 which gives us infinitely many primes p ($p \equiv 1 \bmod 3$) for which we have counterexamples, for $n = 12$.

If $k = 5$, Cook [20] has shown that $n \geq 31$ variables are sufficient, except possibly for $p = 11$, in which case he could only show $n \geq 41$ for a solution; see Cook [21]. Consideration of two disjoint copies of (1.8), in a total of 30 variables show that the best possible result covering all primes would be $n \geq 31$.

Davenport and Lewis [26] showed that

$$\begin{cases} n \geq 2k^2+1 & \text{if } k \text{ odd}\\ n \geq 7k^3 & \text{if } k \text{ even}\end{cases}$$

are sufficient for a pair of additive equations in n variables to have a non-trivial p-adic solution.

1.3.5 $r \geq 3$ additive equations

For 3 additive equations there are fewer results. Artin's conjecture asks whether $3k^2+1$ variables are sufficient to ensure non-trivial p-adic solutions for every prime p. In the case $k = 2$ this was proved by Ellison [31]. When $k = 3$, Stevenson [57] showed that except perhaps for $p = 3,7$ $n \geq 28$ variables are sufficient. Atkinson [2] showed that 25 variables are sufficient for non-trivial p-adic solvability except possibly for $p = 3, 7$. Atkinson, Brüdern and Cook [3] proved that $n \geq 22$ variables give a non-trivial p-adic solution except (possibly) for $p = 3, 7, 13, 19, 31, 37$

and 43.

Davenport and Lewis [25] showed that r simultaneous additive equations have p-adic solutions in greater than $[9r^2k\log 3rk]$ variables when k is odd, and $[48r^2k^3\log 3rk^2]$ variables when k is even. These results have been improved upon by Schmidt [55] and Low, Pitman and Wolff [46].

Finally we quote a result of Atkinson, Brudern and Cook [4], which relates strongly to my Theorem in Chapter 5:

Theorem (Atkinson Brüdern and Cook)

Let r, k, n be positive integers with $k > 1$ and $n > 2rk$. Then the system of equations

$$f_i(x) = a_{i1}x_1^k + \cdots + a_{in}x_n^k = 0, \qquad i = 1, ..., r \tag{1.10}$$

with coefficients $a_{ij} \in \mathbb{Z}$, has a non-trivial p-adic solution for all $p > k^{2r+2}$.

Chapter 2

P-adic normalization

As indicated in Chapter 1, the field of p-adic numbers is not very easy to work with and it is preferable to reduce our search to solutions over the finite field $\mathbb{F}_p$. This we do using Hensel's Lemma which for a system of r diagonal equations

$$f_i(x) = a_{i1}x_1^k + \cdots + a_{in}x_n^k = 0, \qquad i = 1, \ldots, r \tag{2.1}$$

adopts the following form:

Lemma 6 *Let p denote a fixed odd prime number. Let p^τ be the exact power of p which divides k. Then the equations (2.1) will have a non-trivial solution provided that the congruences*

$$f_i(\mathbf{x}) \equiv 0 \bmod p^{\tau+1}, \qquad i = 1, \ldots, r \tag{2.2}$$

have a solution of rank r, where a solution $\mathbf{x} = (x_1, \ldots, x_n)$ has rank s if the matrix $(a_{ij}x_j)$ has rank s mod p.

The proof is almost identical to that of Theorem 1 of the introduction. It is essentially Lemma 9 of Davenport and Lewis [25].

Now we use the technique of p-adic normalization in order to solve the congruences (2.2). This technique is closely connected with the counterexamples in Chapter 1, and attempts to draw out powers of p from the equations.

Two systems of additive forms $f_1, \ldots, f_r$ and $g_1, \ldots, g_r$ are said to be p-equivalent if one system can be obtained from the other by a combination of the operations

$$f_i'(\mathbf{x}) = f_i(p^{v(1)}x_1, \ldots, p^{v(n)}x_n) \text{ for } 1 \leq i \leq r,$$

where $v(1), \ldots, v(n)$ are integers; and

$$f_i''(\mathbf{x}) = \alpha_{i1}f_1(x) + \ldots + \alpha_{ir}f_r(x) \text{ for } 1 \leq i \leq r,$$

where the α_{ij} are rational integers with $\det(\alpha_{ij}) \neq 0$. If $f_1, \ldots, f_r$ have a simultaneous non-trivial zero in the p-adic field then so does any p-equivalent system. Following Davenport and Lewis [25] we introduce the parameter

$$\theta(f_1, \ldots, f_r) = \prod_J \det \mathbf{A}_J,$$

where $\mathbf{A}_J = (a_{ij})$, $1 \leq i \leq r$, $j \in J$, is an $r \times r$ submatrix of A and J runs over all r-element subsets of $\{1, 2, \ldots, n\}$. As in Davenport and Lewis [25] a p-adic compactness argument shows that we may assume that $\theta(f_1, \ldots, f_r) \neq 0$ since if $\theta = 0$ we can choose sequences of forms $f_1^\kappa, \ldots, f_r^\kappa$ converging to $f_1, \ldots, f_r$ p-adically and with $\theta(f_1^\kappa, \ldots, f_r^\kappa) \neq 0$.

We may now assume that $\theta \neq 0$, a property that is preserved under p-equivalence. From all the systems of forms that are p-equivalent to $f_1, \ldots, f_r$, and so have $\theta \neq 0$, and have integral coordinates we select a system $F_1, \ldots, F_r$ for which the power of p dividing $\theta(F_1, \ldots, F_r)$ is least. Such a system of forms is said to be p-normalized. Then we have the following lemma, which is lemma 11 of Davenport and Lewis [25].

Lemma 7 *Suppose that $\mathbf{F}_1, \ldots, \mathbf{F}_r$ is a p-normalized system, with $\theta \neq 0$. Then we may write (after renumbering the variables)*

$$\mathbf{F}_\ell = \mathbf{F}_{\ell,0} + p\mathbf{F}_{\ell,1}, \ 1 \leq \ell \leq r,$$

where

$$\mathbf{F}_{\ell,0} = \alpha_{\ell 1}x_1^k + \cdots + \alpha_{\ell m}x_m^k,$$

$a_{ij} \in \mathbb{Z}$ and each of $x_1, \ldots, x_m$ occurs in at least one of $\mathbf{F}_{1,0}, \ldots, \mathbf{F}_{r,0}$ with a coefficient not divisible by p. Also

$$m \geq \frac{n}{k}.$$

Further, if we form any v linear combinations of the $\mathbf{F}_{\ell,0}$ which are independent mod p, *and denote by q_v the number of variables which occur in at least one of these combinations with a coefficient not divisible by p, then*

$$q_v \geq \frac{vn}{rk}, \ 1 \leq v \leq r-1.$$

Thus we have reduced the p-adic problem to finding a non-singular solution to a set of congruences whose coefficient matrix is reasonably non-singular as defined by the inequalities for the q_v's.

In the next chapter we shall look at the next step in the solution, namely solving the congruences by counting solutions with exponential sums.

Chapter 3

Exponential Sums and the Riemann Hypothesis

3.1 Counting solutions with exponential sums

In this chapter we shall introduce the standard method of exponential sums for counting the number of solutions to equations defined over a finite field.

Let $\{f_1(\mathbf{x}), \ldots, f_r(\mathbf{x})\}$ be any set of polynomials $\mathbb{F}_q^n \to \mathbb{F}_q$, and let N be the number of distinct simultaneous solutions to

$$f_i(\mathbf{x}) = 0, \qquad i = 1, \ldots, r$$

over $\mathbb{F}_q$. Then the key to evaluating N is contained in the following lemma:

Lemma 8

$$q^r N = \sum_{\mathbf{x} \in \mathbb{F}_q^n} \sum_{\mathbf{u} \in \mathbb{F}_q^r} \prod_{i=1}^{r} \psi\left(u_i f_i(\mathbf{x})\right),$$

where ψ is a non-principal additive character of $\mathbb{F}_q$.

Proof. It is a well-known fact that

$$\sum_{\lambda=1}^{q} \psi(\lambda x) = \begin{cases} 0 & \text{if } x \neq 0 \\ q & \text{if } x = 0 \end{cases}.$$

Hence, if we split over $\mathbf{x} \in \mathbb{F}_q^n$ into two parts: those x which are zeros of the f_i's and those which are not, the former count q^r, the latter 0. Hence the result. ■

Now if we take the f_i's to be diagonal equations

$$f_i(\mathbf{x}) = a_{i1}x_1^k + \cdots + a_{in}x_n^k,$$

we can use this result to obtain a very elegant expression for N.

Theorem 9 *Let N be the number of distinct solutions to the system of diagonal equations*

$$f_i(\mathbf{x}) = a_{i1}x_1^k + \cdots + a_{in}x_n^k = 0, \qquad i = 1, \ldots, r \tag{3.1}$$

then

$$q^r N = \sum_{\mathbf{u} \in \mathbb{F}_q^r} \prod_{j=1}^{n} T(L_j(\mathbf{u})) \tag{3.2}$$

where $T(v) = \sum_{x \in \mathbb{F}_q} \psi\left(x^k v\right)$ and $L_j(\mathbf{u}) = \sum_{i=1}^{r} a_{ij}u_i$.

Proof. We begin with

$$q^r N = \sum_{\mathbf{x} \in \mathbb{F}_q^n} \sum_{\mathbf{u} \in \mathbb{F}_q^r} \prod_{i=1}^{r} \psi(u_i f_i(\mathbf{x}))$$

from lemma 8. Introducing diagonal equations as defined in (3.1) gives

$$\begin{aligned} q^r N &= \sum_{\mathbf{x} \in \mathbb{F}_q^n} \sum_{\mathbf{u} \in \mathbb{F}_q^r} \prod_{i=1}^{r} \psi\left(u_i \left[a_{i1}x_1^k + \cdots + a_{in}x_n^k\right]\right) \\ &= \sum_{\mathbf{u} \in \mathbb{F}_q^r} \sum_{\mathbf{x} \in \mathbb{F}_q^n} \prod_{j=1}^{n} \prod_{i=1}^{r} \psi\left(u_i a_{ij} x_j^k\right) \\ &= \sum_{\mathbf{u} \in \mathbb{F}_q^r} \prod_{j=1}^{n} \sum_{x_j \in \mathbb{F}_q^n} \psi\left(\sum_{i=1}^{r} u_i a_{ij} x_j^k\right) \end{aligned}$$

$$
\begin{aligned}
&= \sum_{\mathbf{u}\in\mathbb{F}_q^r} \prod_{j=1}^{n} \sum_{\mathbf{x}_j\in\mathbb{F}_q^n} \psi\left(x_j^k \sum_{i=1}^{r} u_i a_{ij}\right) \\
&= \sum_{\mathbf{u}\in\mathbb{F}_q^r} \prod_{j=1}^{n} \sum_{\mathbf{x}\in\mathbb{F}_q^n} \psi\left(x^k \sum_{i=1}^{r} a_{ij} u_i\right) \\
&= \sum_{\mathbf{u}\in\mathbb{F}_q^r} \prod_{j=1}^{n} T(L_j(\mathbf{u})).
\end{aligned}
$$

■

We can then proceed by isolating the term from the sum due to $\mathbf{u} = \mathbf{0}$, giving, on dividing by q^r,

$$
N - q^{n-r} = \frac{1}{q^r} \sum_{\mathbf{0}\neq\mathbf{u}\in\mathbb{F}_q^r} \prod_{i=1}^{r} T(L_i(\mathbf{u})). \tag{3.3}
$$

Most methods then take the modulus of both sides and try to show that $|N - q^{n-r}| = o(q^{n-r})$, implying that $N > 0$ for large enough q. For example, observing that in general $n - r$ is the dimension of the solution space of (3.1), we see that the theorem of Lang-Weil would give us, under suitable conditions on the a_{ij},

$$
|N - q^{n-r}| \leq c q^{n-r-\frac{1}{2}},
$$

for some constant c, giving us a solution for $q > c^2$.

In chapter 4 we demonstrate a new method which uses multiplicative instead of additive characters. (A multiplicative character χ of $\mathbb{F}_q$ is a homomorphism from the multiplicative group $\mathbb{F}_q^*$ to $\mathbb{C}$, together with the condition $\chi(0) = 0$). We use it to solve a pair of additive equations, but it can easily be extended to cover more than two.

Basically we introduce multiplicative characters into (3.3) using the following lemma:

Lemma 10 *If p does not divide Λ then*

$$
T(\Lambda) = \sum_{r=1}^{k-1} \chi^r(\Lambda)\tau(\overline{\chi}^r),
$$

where χ is a non-principal character of order k, and τ is the Gaussian sum

$$\tau(\chi) = \sum_{x=1}^{p} \chi(x) e\left(\frac{x}{p}\right).$$

This is Lemma 4.3 of Vaughan [61].

We can then use the fact that

$$|\tau(\overline{\chi}^r)| = \sqrt{p}, \text{ for } 1 \leq r \leq k-1$$

and the celebrated Hasse-Weil character sum estimate to give a very sharp estimate for the difference. For more than two equations we need a character sum estimate similar to the Hasse-Weil, but in more than one variable. As we shall see later this generalised Hasse-Weil estimate has applications, not only for diagonal equations, but also in Graph Theory. We examine the possibilities of such a result next.

3.2 Extending the Hasse-Weil estimate

The Hasse-Weil character sum estimate is the following theorem:

Lemma 11 (Hasse-Weil) *Let p be a prime number and let χ be any non-principal character (mod p) of order k, where k divides $(p-1)$. Let $B(x)$ be a polynomial of the form*

$$(x-a_1)^{\alpha_1} \ldots (x-a_t)^{\alpha_t},$$

where the a_i are all distinct (mod p), and $0 < \alpha_i < k$.

Then,

$$\left| \sum_{x \bmod p} \chi(B(x)) \right| \leq (t-1)\sqrt{p}$$

where the summation is over a complete set of residues mod p.

For an elementary proof see [45], chapters 5 and 6.

The Hasse-Weil character sum involves estimating a sum of the form

$$\sum_{\mathbb{F}_q} \chi(f(x))$$

where χ is a multiplicative character of order k and f is a polynomial given by a product of powers of t linear forms in one variable. An obvious generalisation of this to more than one variable would be to take f to be a product of powers of linear forms in $n > 1$ variables say. In this chapter we wish to look at this case and conjecture a suitable theorem.

3.3 Zeta functions and the Riemann hypothesis over finite fields

Let $S = \{f_1 = 0, \ldots, f_r = 0\}$ be any set of polynomial equations over a finite field $\mathbb{F}_q$, q a power of some prime p. Let $H(K)$ be the solution set of S over some field K containing $\mathbb{F}_q$. Then define $N_s = \#(H(\mathbb{F}_{q^s}))$, $\mathbb{F}_{q^s}$ being a finite algebraic extension of $\mathbb{F}_q$ of degree s.

Given any such sequence of $\{N_s\}$ we can consider a type of generating function, encoding the information in $\{N_s\}$ in the form of a power series. This is known as the Hasse-Weil zeta function of S, defined by

$$\exp\left(\sum_{s=1}^{\infty} N_s \frac{T^s}{s}\right) \in \mathbb{Q}\left[[T]\right].$$

This is usually written as $Z(H/\mathbb{F}_q; T)$. We have the following theorem proved by Dwork [30] using p-adic analysis.

Theorem 12 *(Dwork). The zeta-function of any affine (or projective) variety is a ratio of two polynomials with coefficients in $\mathbb{Z}$ and constant term 1.*

Dwork's theorem has profound implications for the solution of polynomial equations over finite fields. It implies that there exist a finite set of complex numbers $\alpha_1, \ldots, \alpha_n$ such that for all $s = 1, 2, 3, \ldots$ we have $N_s = \sum_{i=1}^{t} \alpha_i^s - \sum_{i=t+1}^{n} \alpha_i^s$. In fact the α's are the roots and poles of the zeta function. (See Katz [40]). Much more information can be obtained about these, including bounds on t and u. In fact in 1949 [64] , Weil conjectured the following:

Let X be an n-dimensional projective non-singular variety over $\mathbb{F}_q$. Then

1. $Z(X/\mathbb{F}_q, T)$ is a rational function of T.

2. Moreover, $Z(X/\mathbb{F}_q, T) = \dfrac{P_1(T)\ P_3(T)\ \ldots\ P_{2n-1}(T)}{P_0(T)\ P_2(T)\ \ldots\ P_{2n}(T)}$, where $P_i(T) = \prod_{j=1}^{b_i}(1-\alpha_{ij}T)$, $\quad |\alpha_{ij}| = q^{\frac{i}{2}}$, the last equality being the 'Riemann hypothesis' in this setting.

3. Under $\alpha \longmapsto q^n/\alpha$, the α_{ij} are carried bijectively to the $\alpha_{2n-i\,j}$. In terms of the complex variable s, this is a functional equation for $s \longmapsto n - s$.

4. In case X is the 'reduction modulo p ' of a non-singular projective variety $\mathbb{X}$ in characteristic zero, then b_i is the i'th topological Betti number of $\mathbb{X}$ as a complex manifold.

These conjectures have now been proved in full, the extremely difficult 2. having been settled by Pierre Deligne in 1974 [28].

3.4 The case of character sums

Let E be an extension field of $\mathbb{F}_q$ of degree s, then $E = \mathbb{F}_{q^s}$. We note that χ can be lifted to a multiplicative character $\chi^{(s)}$ of the extension E by setting $\chi^{(s)}(\beta) = \chi(\mathrm{N}_{E/\mathbb{F}_q}(\beta))$ for $\beta \in E$.

A zeta function can be defined and corresponding Weil conjectures formulated for character sums, giving us $\sum_{\gamma\in\mathbb{F}_q}\chi^{(s)}(f(\gamma)) = \sum_{i=1}^{t}\alpha_i^s - \sum_{i=t+1}^{c}\alpha_i^s$ for some c and complex numbers α_i. In fact Perelmutter [50], [51] has looked at the case $k = 2$ when f and its leading form f_d, the terms of degree d in f, satisfy certain natural conditions:

1. Over $\overline{\mathbb{F}}_q$ the system of equations $\left\{f(\mathbf{x}) = \frac{\partial f(\mathbf{x})}{\partial x_1} = \cdots = \frac{\partial f(\mathbf{x})}{\partial x_n} = 0\right\}$ has no solution.

2. Over $\overline{\mathbb{F}}_q$ the system of equations $\left\{f_d(\mathbf{x}) = \frac{\partial f_d(\mathbf{x})}{\partial x_1} = \cdots = \frac{\partial f_d(\mathbf{x})}{\partial x_n} = 0\right\}$ has no solution other than the trivial one $x_1 = \ldots = x_n = 0$.

The geometric significance of these conditions is that the variety defined by f is non-singular and also has no singular points at infinity. In this case he obtains

$$\left|\sum_{\mathbb{F}_q^n}\chi(f(x_1,\ldots,x_n))\right| \leq (t-1)^n q^{\frac{n}{2}}$$

for the character sum. Unfortunately if f is a product of powers of linear forms it does not satisfy these conditions. In fact the variety one considers is singular, preventing the direct

application of the Weil conjectures. However, in a personal communication, Professor N. Katz has suggested that, using the techniques of perverse sheaves and l-adic Fourier transforms, one should be able to prove $\left|\sum_{\gamma\in\mathbb{F}_q}\chi^{(s)}(f(\gamma))\right| \leq cq^{\frac{sn}{2}}$ for some constant c, and almost all forms f of the type we are considering. This means that if $\sum_{\gamma\in\mathbb{F}_q}\chi^{(s)}(f(\gamma)) = \sum_{i=1}^{t}\alpha_i^s - \sum_{i=t+1}^{c}\alpha_i^s$, the $\alpha_i's$ must satisfy $|\alpha_i| \leq q^{\frac{n}{2}}$. This constitutes the first step in deriving our character sum estimate. The second requires a bound on the constant c.

The constant c will almost certainly depend on the linear dependence between the forms. Let us consider $f(\mathbf{x}) = \prod_{i=1}^{l} f_i(x_i)$, where $f_i = \prod_{j=1}^{n_i}(x_i - a_{ij})^{r_{ij}}, 0 < r_{ij} < k$ and a_{ij} all distinct for fixed i. Thus each f_i is a polynomial in x_i, a product of n_j linear forms in 1 variable with $r_{ij} \neq 0 \bmod k$. Also by the Hasse-Weil character sum estimate we have

$$\left|\sum_{x_i=1}^{q}\chi\left(f_i(x_i)\right)\right| = \left|\sum_{x_i=1}^{q}\chi\left(\prod_{j=1}^{n_i}(x_i - a_{ij})^{r_{ij}}\right)\right| \leq n_i q^{\frac{1}{2}}.$$

Thus we obtain

$$\left|\sum_{\mathbf{x}\in\mathbb{F}_q^l}\chi(f(\mathbf{x}))\right| = \prod_{i=1}^{l}\left|\sum_{x_i=1}^{q}\chi\left(f_i(x_i)\right)\right| \leq n_1 n_2 \ldots n_l q^{\frac{l}{2}},$$

with $n_1 + n_2 + \ldots + n_l = n$ where f is a product of n linear forms, in l variables. In order to produce a uniform bound depending on n and l only we use the arithmetic mean - geometric mean inequality giving

$$n_1 n_2 \ldots n_l \leq \left(\frac{n_1 + n_2 + \ldots + n_l}{l}\right)^l = \left(\frac{n}{l}\right)^l.$$

So,

$$\left|\sum_{\mathbf{x}\in\mathbb{F}_q^l}\chi(f(\mathbf{x}))\right| \leq \left(\frac{n}{l}\right)^l q^{\frac{l}{2}}.$$

We wish this to be consistent with the case where f is the product of t disjoint polynomials, f_i, where each f_i is the product of n_i powers of linear forms in l_i variables. In this case, applying the estimate for each f_i separately gives

$$\left|\sum_{\mathbf{x}\in\mathbb{F}_q^l}\chi(f(\mathbf{x}))\right| = \prod_{i=1}^{t}\left|\sum_{x}\chi\left(f_i(x)\right)\right| \leq \prod_{i=1}^{t}\left(\frac{n_i}{l_i}\right)^{l_i} q^{\frac{l}{2}}$$

where $l = l_1 + \cdots + l_t$. For this result to be consistent with applying the conjecture to the whole of f as a product of $n = n_1 + n_2 + \ldots + n_l$ linear forms, in l variables, we need

$$\prod_{i=1}^{t} \left(\frac{n_i}{l_i}\right)^{l_i} \leq \left(\frac{n}{l}\right)^{l}. \tag{3.4}$$

This is obtained by using the inequality of the means with the values $\frac{n_i}{l_i}$, each taken l_i times, $1 \leq i \leq t$, giving

$$\left(\frac{n}{l}\right) = \frac{1}{l}\sum_{i=1}^{t}\left(\frac{n_i}{l_i} \times l_i\right) \geq \left(\prod_{i=1}^{t}\left(\frac{n_i}{l_i}\right)^{l_i}\right)^{\frac{1}{l}}$$

and hence 3.4. Thus we take $\left(\frac{n}{l}\right)^l$ as a uniform bound on the constant c. We note however that for polynomials f whose linear forms are not as singular as our example, the value of c will probably be much lower.

We call f *non-degenerate* with respect to the multiplicative character χ if the character sum $\sum_{\mathbf{F}_q^n} \chi(f(x_1, \ldots, x_n))$ cannot be reduced by a non-singular rational change of variables to one in fewer variables. As the following example shows, if the conjecture concerning the $\alpha_i's$ is to be correct we must make the additional assumption that f is non-degenerate with respect to χ.

Example 13

$$\begin{aligned}\sum_{x,y}\chi(x(x+y)(x+2y)(x+5y)) &= \sum_{x,y\neq 0}\chi(y(x+y)(x+2y)(x+5y)) \\ &= \sum_{x,y\neq 0}\chi(y^4(\frac{x}{y}+1)(\frac{x}{y}+2)(\frac{x}{y}+5)) \\ &= \sum_{u,y\neq 0}\chi((u+1)(u+2)(u+5)) \\ &= (q-1)\sum_{u}\chi((u+1)(u+2)(u+5)).\end{aligned}$$

since $\chi(y^4) = 1$ as χ is of order 2. Thus using the Hasse-Weil esimate we can only obtain

$$\begin{aligned}\left|\sum_{x,y}\chi(x(x+y)(x+2y)(x+5y))\right| &= (q-1)\left|\sum_{u}\chi((u+1)(u+2)(u+5))\right| \\ &\leq 2(q-1)q^{\frac{1}{2}}.\end{aligned}$$

Thus we have incurred a factor of $\sqrt{q}$ for the variable y which we managed to eliminate.

3.5 The main conjecture

Conjecture 14 *Let χ be a multiplicative character of $\mathbb{F}_q$ of order $k > 1$ and let $f \in \Phi$ be a polynomial in m variables which is non-degenerate, and is the product of d distinct linear forms with multiplicities $r_1, \ldots, r_d$ over $\overline{\mathbb{F}}_q$, such that $0 < r_i < k$. Then we have:*

$$\sum_{\gamma \in \mathbb{F}_q} \chi(f(\gamma)) \leq \left(\frac{d}{m}\right)^m q^{\frac{m}{2}}.$$

3.5.1 Non-degeneracy of f

Let us consider a polynomial $f = \prod_{i=1}^{t} f_i^{r_i}$, where $f_i = \sum_{j=1}^{n} a_{ij}x_j + a_{in+1}$. We wish to relate the degeneracy of f to the matrix $A = (a_{ij})$.

f is non-degenerate if and only if A has rank $n+1$ and the set of column vectors cannot be decomposed into r sets, with $r \geq 2$, whose spans intersect only in the zero vector. This basically means that there is no row operation on the matrix which takes it to a form consisting of r disjoint blocks with $r \geq 2$. Alternatively we can say that there is no rational transformation of coordinates that takes f to a form f' where f' is a product of two or more disjoint forms.

Example 15 *The matrix* $A = \begin{pmatrix} 1 & 0 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 0 & 1 & 2 \end{pmatrix}$ *would represent a degenerate polynomial since the first three vectors lie in one 2-dimensional subspace and the remaining three lie in another disjoint 2-dimensional subspace.*

We also note that from the rank-nullity theorem for linear transformations, the rank of A is equal to $n+1-\dim K$, where K is the solution set of $F_i = 0$, $1 \leq i \leq t$, where the homogeneous linear form F_i is given by

$$F_i = \sum_{j=1}^{n+1} a_{ij}x_j.$$

3.5.2 Homogeneous polynomials

We will now consider the case where f is a homogeneous polynomial, as this will be useful for our applications to graph theory in a later chapter.

Connected forms

We call a homogeneous form *connected* if it is not equal to the product of two disjoint forms. Thus we see that the condition for f to be non-degenerate can be expressed as: f is non-degenerate if and only if A has rank $n+1$ and f is connected.

If a form is not connected then it is *disconnected* and it has a unique expression as a product of connected forms. Each form is then called a *component* and the total number of components is called the *connectivity* of f. If a form f is connected we say it has connectivity 1.

Estimate for a connected homogeneous form

Let $f = \prod_{i=1}^{t} f_i^{r_i}$, where f is connected and the $f_i = \sum_{j=1}^{n} a_{ij}x_j$, a product of powers of linear homogeneous polynomials . As before, the most important fact about f is the rank of $A = (a_{ij})$. If rank $A = n - \rho$ then there is a non-singular linear transformation which is a bijection and takes A to a matrix with the bottom ρ rows zero. Thus $f(x_1, \ldots, x_n) = g(w_1, \ldots, w_n)$ where $g = \prod_{i=1}^{t} g_i^{r_i}$, and $g_i = \sum_{j=1}^{n-\rho} b_{ij}w_j$. Also we may assume by elementary row operations and relabling that $g_{n-\rho} = w_{n-\rho}$.

Hence,

$$\sum_{\mathbf{x}\in\mathbb{F}_q^n} \chi(f(\mathbf{x})) = \sum_{\mathbf{w}\in\mathbb{F}_q^n} \chi(g(\mathbf{w})) = q^{\rho} \sum_{\mathbf{w}'\in\mathbb{F}_q^{n-\rho}} \chi(g(\mathbf{w}')),$$

where $w' = (w_1, \ldots, w_{n-\rho})$.

We now split $\mathbb{F}_q^{n-\rho}$ into two disjoint sets,

$$\begin{aligned} W_1 &= \left\{(w_1, \ldots, w_{n-\rho}) \in \mathbb{F}_q^{n-\rho} : w_{n-\rho} \neq 0\right\} \\ W_2 &= \left\{(w_1, \ldots, w_{n-\rho}) \in \mathbb{F}_q^{n-\rho} : w_{n-\rho} = 0\right\}. \end{aligned}$$

Then, since $g(w) = 0$ for all $w \in W_2$,

$$\begin{aligned} \sum_{\mathbf{w}\in\mathbb{F}_q^{n-\rho}} \chi(g(\mathbf{w})) &= \sum_{\mathbf{w}\in W_1} \chi(g(\mathbf{w})) + \sum_{\mathbf{w}\in W_2} \chi(g(\mathbf{w})) \\ &= \sum_{\mathbf{w}\in W_1} \chi(g(\mathbf{w})). \end{aligned}$$

Now if $w_{n-\rho} \neq 0$,

$$g_i = w_{n-\rho} \sum_{j=1}^{n-\rho} a_{ij} \frac{w_j}{w_{n-\rho}}.$$

If we make a change of variables

$$v_j = \frac{w_j}{w_{n-\rho}}, 1 \leq j \leq n-\rho-1, v_{n-\rho} = w_{n-\rho}$$

then $g(\mathbf{w})|_{W_1} = h(v_1, \ldots, v_{n-\rho})$ where $h = v_{n-\rho}^{\sum_{i=1}^{t} r_i} \prod_{i=1}^{t-1} h_i^{r_i}$ and $h_i = \sum_{j=1}^{n-\rho-1} a_{ij} v_j + a_{in-\rho}$.

Hence,

$$\begin{aligned} \sum_{\mathbf{w} \in \mathbf{W}_1} \chi(g(\mathbf{w})) &= \sum_{\mathbf{v} \in \mathbf{W}_1} \chi(h(\mathbf{v})) = \sum_{\mathbf{v} \in \mathbf{W}_1} \chi(v_{n-\rho}^{\sum_{i=1}^{t} r_i} \prod_{i=1}^{t-1} h_i^{r_i}) \\ &= \sum_{\mathbf{v}_{n-\rho}=1}^{p-1} \chi(v_{n-\rho}^{\sum_{i=1}^{t} r_i}) \times \sum_{v_1=1}^{p} \cdots \sum_{v_{n-\rho-1}=1}^{p} \chi(\prod_{i=1}^{t-1} h_i^{r_i}). \end{aligned}$$

If we let $R = \sum_{i=1}^{t} r_i$ then

$$\sum_{\mathbf{v}_{n-\rho}=1}^{p-1} \chi(v_{n-\rho}^{\sum_{i=1}^{t} r_i}) = \begin{cases} 0 & \text{if } R \neq 0 \pmod{k} \\ q-1 & \text{if } R \equiv 0 \pmod{k} \end{cases}.$$

Now obviously since g has rank $n-\rho$ and is connected, g is non-degenerate. Hence $\prod_{i=1}^{t} h_i^{r_i}$ is non-degenerate so we may apply the conjecture with $m = n-\rho-1$ and $d = t-1$ to give

$$\left| \sum_{v_1=1}^{p} \cdots \sum_{v_{n-\rho-1}=1}^{p} \chi(\prod_{i=1}^{t-1} h_i^{r_i}) \right| \leq \left(\frac{t-1}{n-\rho-1} \right)^{n-\rho-1} q^{\frac{n-\rho-1}{2}}.$$

Hence

$$\left| \sum_{\mathbf{w} \in \mathbf{W}_1} \chi(g(\mathbf{w})) \right| = \leq \begin{cases} 0 & \text{if } R \neq 0 \pmod{k} \\ (q-1) \left(\frac{t-1}{n-\rho-1} \right)^{n-\rho-1} q^{\frac{n-\rho-1}{2}} & \text{if } R \equiv 0 \pmod{k} \end{cases}.$$

This gives

$$\left|\sum_{\mathbf{x}\in\mathbf{F}_q^n}\chi(f(\mathbf{x}))\right| = \begin{cases} 0 & if \quad R\neq 0 \pmod k \\ \leq (q-1)\left(\frac{t-1}{n-\rho-1}\right)^{n-\rho-1} q^{\frac{n+\rho-1}{2}} & \text{if} \quad R\equiv 0 \pmod k \end{cases} . \tag{3.5}$$

Part II

Diagonal p-adic Equations

Chapter 4

Pairs of Additive Equations[1]

4.1 Introduction

It is well known that the number of solutions of polynomial congruences can be estimated using exponential sums. This is usually an essential prerequisite to establishing non-trivial p-adic solutions to sets of forms via Hensel's Lemma. In this chapter we are concerned with the problem of establishing good bounds on the primes p for which a p-adic solution is possible for a fixed number of variables. As we have noted in the survey, with regard to the latter problem, Atkinson, Brüdern and Cook [4] proved the following result which we repeat for convenience:

Theorem *(Atkinson,Brüdern and Cook)*
Let r, k, n be positive integers with $k > 1$ and $n > 2rk$. Then the system of equations

$$F_i(x) = a_{i1}x_1^k + \cdots + a_{in}x_n^k = 0, \qquad i = 1, ..., r$$

with coefficients $a_{ij} \in \mathbb{Z}$, has a non-trivial p-adic solution for all $p > k^{2r+2}$.

In the case of two additive equations, $r = 2$, the theorem guarantees a non-trivial solution for all $p > k^6$, with $n > 4k$ variables. See also [5].

[1] **The contents of this chapter have been accepted for publication in the Journal of Number Theory.**

The aim of this chapter is to improve the bound to $p > 3k^4$. The result involves a considerable modification of the standard method of exponential sums. We use a character sum estimate for a polynomial in one variable. This follows from the results of H.Hasse on the analogue L-functions belonging to a certain algebraic number field, and the deep theorem of A.Weil that the congruence zeta function that this L-function divides has all its roots on the critical line.

The main theorem is:

Theorem 16 *Let n, k be positive integers with $k > 1$, $n > 4k$. Then the system of equations*

$$\begin{aligned} f(x) &= a_1 x_1^k + \cdots + a_n x_n^k = 0 \\ g(x) &= b_1 x_1^k + \cdots + b_n x_n^k = 0 \end{aligned} \tag{4.1}$$

with coefficients a_i, $b_i \in \mathbb{Z}$, has a non-trivial p-adic solution for all $p > 3k^4$.

As usual we must begin by reducing the solution in p-adic integers to a solution of certain congruences mod p. This we do in the preliminaries to Theorem 16, in which we follow very closely the preliminaries in [5].

4.2 Preliminaries to Theorem 16

We begin by recalling the normalization procedure introduced in chapter 2. With a pair of additive forms f, g (4.1) we associate the parameter

$$\theta = \theta(f, g) = \prod_{i \neq j} (a_i b_j - b_i a_j) .$$

For a given pair of forms with $\theta(f, g) \neq 0$ and a fixed prime p, there is a related p-normalized pair of forms (f^*, g^*). Further the equations $f = g = 0$ have a non-trivial p-adic solution if and only if the equations $f^* = g^* = 0$ do. Also, by the p-adic compactness argument in Davenport and Lewis [24], it is sufficient to prove Theorem 16 with the additional assumption that $\theta \neq 0$, and use the following property which is essentially Lemma 2 of Davenport and Lewis [24], and our Lemma 7 from Chapter 2.

Lemma 17 *Let f and g be a p-normalized pair of forms. Then we may write*

$$\begin{aligned} f &= f_0 + pf_1 \\ g &= g_0 + pg_1. \end{aligned}$$

Here f_0, g_0 are forms in $m \geq n/k$ variables, each of which occurs in at least one of f_0, g_0 with a coefficient not divisible by p. Further, if q denotes the minimum number of variables occurring explicitly in any form $\lambda f_0 + \mu g_0$ (λ, μ not both divisible by p) with a coefficient not divisible by p, then $q \geq n/2k$.

Our next lemma is a version of Hensel's Lemma given as Lemma 6 in Chapter 2; it is Lemma 7 of Davenport and Lewis [26].

Lemma 18 *If odd p does not divide k and the congruences*

$$\begin{aligned} f_0 = a_1 x_1^k + \cdots + a_m x_m^k &\equiv 0 \pmod{p} \\ g_0 = b_1 x_1^k + \cdots + b_m x_m^k &\equiv 0 \pmod{p} \end{aligned} \tag{4.2}$$

have a solution $\xi = (\xi_1, \ldots, \xi_m)$ for which the matrix

$$\begin{pmatrix} a_1\xi_1, \ldots, a_m\xi_m \\ b_1\xi_1, \ldots, b_m\xi_m \end{pmatrix}$$

has rank 2 (mod p) then the equations $f_0 = g_0 = 0$ have a non-trivial solution in p-adic integers.

In the proof of Theorem 16 we have $p > 3k^4$, so $(p, k) = 1$. It is therefore sufficient to show that the congruences (4.2) have a solution of rank 2. We may also suppose that $p \equiv 1 \pmod{k}$ since otherwise all residues are kth powers and the congruences (4.2) reduce to two linear equations and the solutions are obtained by simple linear algebra.

Since $n > 4k$, Lemma 17 gives the bounds $m \geq 5$, $q \geq 3$. We partition the variables $x_1, \ldots, x_m$ into blocks such that in each block the ratios a_i/b_i are equal (mod p). Let ρ be the length of the longest block of common ratios a_i/b_i. We note that replacing f_0, g_0 by suitable linear combinations we may take $a_i/b_i =$ '1/0' for these ρ variables. Further, let t be the length of the second longest block of common ratios. We may take the ratios in this block to be '0/1'.

We assert that if $t \geq 3$ then the congruences (4.2) have a common solution of rank 2. We know that a single congruence $ax^k + by^k + cz^k \equiv 0 \pmod{p}$, $(p, abc) = 1$, has a non-trivial solution for all $p > k^4$ (see Theorem 1 of Chowla [18]), so our assertion follows from the fact that the congruences (4.2) contain two distinct congruences in 3 variables. Now we assume that $t \leq 2$ and reduce m from its initial value to 5 by discarding variables from the longest block of common ratios. We end up with a pair of congruences (4.2) satisfying

$$m = 5, \ q \geq 3 \text{ and } \rho \leq 2, \tag{4.3}$$

since $\rho = m - q$. To ensure a non-trivial p-adic solution we require that the solution is of rank 2. We split the proof into two parts, $\rho = 1$ and $\rho = 2$.

4.3 Important definitions and lemmas

Definition 19 *Let $\Lambda = ua_i + vb_i$ be a linear form in u, v and define*

$$T(\Lambda) = \sum_{x=1}^{p} e_p\left(\Lambda x^k\right), \tag{4.4}$$

where

$$e_p(x) = \exp\left(\frac{2\pi i x}{p}\right).$$

Lemma 20 *If p does not divide Λ then*

$$T(\Lambda) = \sum_{r=1}^{k-1} \chi^r(\Lambda)\tau(\overline{\chi}^r),$$

where χ is a non-principal character of order k, and τ is the Gaussian sum

$$\tau(\chi) = \sum_{x=1}^{p} \chi(x)e_p(x).$$

This is Lemma 4.3 of Vaughan [61].

It is well known that

$$|\tau(\overline{\chi}^r)| = \sqrt{p}, \text{ for } 1 \leq r \leq k-1. \tag{4.5}$$

Lemma 21 (Hasse-Weil) *Let p be a prime number and let χ be any non-principal character (mod p) of order k, where k divides $(p-1)$. Let $B(x)$ be a polynomial of the form*

$$(x-a_1)^{\alpha_1}\dots(x-a_t)^{\alpha_t},$$

where the a_i are all distinct (mod p), and $0<\alpha_i<k$.

Then,

$$\left|\sum_{x \bmod p}\chi(B(x))\right| \le (t-1)\sqrt{p},$$

where the summation is over a complete set of residues mod p.

For an elementary proof see [45], chapters 5 and 6.

Lemma 22 *Let χ be a non-principal character of order k, $a_i, b_j \in \mathbb{Z}$, with $a_ib_j - a_jb_i \not\equiv 0 \pmod p$ for $i \neq j$, and $a_i \not\equiv 0 \pmod p$ for $i = 1,\dots,t$. Let $r_1,\dots r_t$ be integers such that $0<r_i<k$. Then*

$$\left|\sum_{\lambda=1}^{p-1}\chi\left(\prod_{i=1}^{t}(a_i\lambda+b_i)^{r_i}\right)\right| \le (t-1)\sqrt{p}+1. \tag{4.6}$$

Proof.

Since χ is multiplicative and $a_i \not\equiv 0 \pmod p$ we have

$$\chi\left(\prod_{i=1}^{t}(a_i\lambda+b_i)^{r_i}\right) = \chi\left(a_i^{r_i}\prod_{i=1}^{t}\left(\lambda+\frac{b_i}{a_i}\right)^{r_i}\right) = \chi\left(\prod_{i=1}^{t}a_i^{r_i}\right)\chi\left(\prod_{i=1}^{t}(\lambda+c_i)^{r_i}\right),$$

where the c_i's are distinct because $a_ib_j - a_jb_i \not\equiv 0 \pmod p$, and b_i/a_i is interpreted mod p.

So,

$$\begin{aligned}
&\left|\sum_{\lambda=1}^{p-1}\chi\left(\prod_{i=1}^{t}(a_i\lambda+b_i)^{r_i}\right)\right| = \left|\chi\left(\prod_{i=1}^{t}a_i^{r_i}\right)\sum_{\lambda=1}^{p-1}\chi\left(\prod_{i=1}^{t}(\lambda+c_i)^{r_i}\right)\right| \\
= &\left|\sum_{\lambda=1}^{p-1}\chi\left(\prod_{i=1}^{t}(\lambda+c_i)^{r_i}\right)\right| = \left|\sum_{\lambda=1}^{p}\chi\left(\prod_{i=1}^{t}(\lambda+c_i)^{r_i}\right) - \chi\left(\prod_{i=1}^{t}c_i^{r_i}\right)\right| \\
\le &\left|\sum_{\lambda=1}^{p}\chi\left(\prod_{i=1}^{t}(\lambda+c_i)^{r_i}\right)\right| + 1 \\
\le &\ (t-1)\sqrt{p}+1
\end{aligned} \tag{4.7}$$

by Lemma 21. ■

Lemma 23 *Let* $S_n = \sum_{u=1}^{p-1} |T(u)|^n$, *with* T *as (4.4). Then*

$$|S_n| \leq (k-1)^{n-1} p^{\frac{n}{2}+1}. \tag{4.8}$$

See [5] p.446.

Lemma 24 *Let* $p \equiv 1 \pmod{k}$, $p > k^4$. *If* $abc \not\equiv 0 \pmod{p}$, *then the congruence*

$$ax^k + by^k + cz^k \equiv d \pmod{p} \tag{4.9}$$

has a solution with $xyz \not\equiv 0 \pmod{p}$.

Proof.

We count the number N_1 of solutions of (24) using exponential sums,

$$pN_1 = \sum_u T(au)T(bu)T(cu)e\left(\frac{-du}{p}\right).$$

Separating out the term $u \equiv 0 \pmod{p}$,

$$\begin{aligned} \left|pN_1 - p^3\right| &\leq \sum_{u \not\equiv 0} |T(au)T(bu)T(cu)| \\ &= \sum_{u=1}^{p-1} |T(au)T(bu)T(cu)| \\ &\leq \left\{ \sum_{u=1}^{p-1} |T(au)|^3 \sum_{u=1}^{p-1} |T(bu)|^3 \sum_{u=1}^{p-1} |T(cu)|^3 \right\}^{\frac{1}{3}}. \end{aligned}$$

As u runs through $1, 2, \ldots, p-1$ so do au, bu and cu. Thus each sum

$$\sum_{u=1}^{p-1} |T(au)|^3 = \sum_{u=1}^{p-1} |T(bu)|^3 = \sum_{u=1}^{p-1} |T(cu)|^3 = S_3.$$

So we have

$$\left|pN_1 - p^3\right| \leq S_3 \leq (k-1)^2 p^{\frac{5}{2}}.$$

When $x \equiv 0 \pmod{p}$, the congruence (24) becomes

$$by^k + cz^k \equiv d \pmod{p}.$$

For any given value of y there are at most k solutions for z, so the number of solutions of (24) with $xyz \equiv 0 \pmod{p}$ is at most $3kp$.

Thus for a solution to (24) with $xyz \not\equiv 0 \pmod{p}$ we require

$$\begin{aligned} p^2 - (k-1)^2 p^{\frac{3}{2}} &> 3kp, \\ p^{\frac{1}{2}} - 3kp^{-\frac{1}{2}} &> (k-1)^2. \end{aligned}$$

Since $p > k^4$ we have, for $k \geq 2$,

$$p^{\frac{1}{2}} - 3kp^{-\frac{1}{2}} > k^2 - \frac{3}{k} > (k-1)^2.$$

Thus $p > k^4$ is sufficient for a solution. ■

4.4 Theorem 16 : the case $\rho = 1$

In this case any non-trivial solution has rank 2 $\pmod{p}$. We begin by using elementary row operations to put the congruences in the form

$$\begin{aligned} f_0 &= x_1^k + \quad a_3 x_3^k + \cdots + a_m x_m^k \equiv 0 \pmod{p} \\ g_0 &= \quad x_2^k + b_3 x_3^k + \cdots + b_m x_m^k \equiv 0 \pmod{p}. \end{aligned} \tag{4.10}$$

The number N of solutions to the congruences (4.10) is given by

$$p^2 N = \sum_{u,v} T(\Lambda_1) \cdots T(\Lambda_5).$$

Taking across the term due to $u = v = 0$, we have

$$p^2 N - p^5 = \sum_{(u,v) \neq (0,0)} T(\Lambda_1) \cdots T(\Lambda_5). \tag{4.11}$$

We now separate the sum into terms for which one of the Λ_i's is zero (mod p), denoted by Σ_1,and terms for which none of the Λ_i's are zero (mod p), denoted by Σ_0 . The estimate of Σ_1 is done in the standard way using Lemma 4.8. The estimate for Σ_0, however, is new and requires Lemma 22.

4.5 Estimate for Σ_0

We substitute the expression for T given in Lemma 20 into Σ_0,

$$\begin{aligned}
\Sigma_0 &= \sum_{\substack{u,v \\ \Lambda_i \not\equiv 0 \ (p)}} \sum_{\substack{r_1,\ldots,r_5 \\ 1 \le r_i \le k-1}} \chi(\Lambda_1^{r_1} \cdots \Lambda_5^{r_5}) \tau(\overline{\chi}^{r_1}) \cdots \tau(\overline{\chi}^{r_5}) \\
&= \sum_{\substack{r_1,\ldots,r_5 \\ 1 \le r_i \le k-1}} \left[\sum_{\substack{u,v \\ \Lambda_i \not\equiv 0 \ (p)}} \chi(\Lambda_1^{r_1} \cdots \Lambda_5^{r_5}) \tau(\overline{\chi}^{r_1}) \cdots \tau(\overline{\chi}^{r_5}) \right] \\
&= \sum_{\substack{r_1,\ldots,r_5 \\ 1 \le r_i \le k-1}} \tau(\overline{\chi}^{r_1}) \cdots \tau(\overline{\chi}^{r_5}) \left[\sum_{\substack{u,v \\ \Lambda_i \not\equiv 0 \ (p)}} \chi(\Lambda_1^{r_1} \cdots \Lambda_5^{r_5}) \right].
\end{aligned}$$

We now fix $r_1, \ldots, r_5$ and evaluate the inner sum.

$$\begin{aligned}
S_0 = \sum_{\substack{u,v \\ \Lambda_i \not\equiv 0 \ (p)}} \chi\left(\prod_{i=1}^{5} \Lambda_i^{r_i}\right) &= \sum_{\substack{u,v \\ \Lambda_i \not\equiv 0 \ (p)}} \chi\left(\prod_{i=1}^{5} (a_i u + b_i v)^{r_i}\right) \\
&= \sum_{\substack{u,v \\ \Lambda_i \not\equiv 0 \ (p)}} \chi\left(v^{r_1+\cdots+r_5} \prod_{i=1}^{5} (a_i \frac{u}{v} + b_i)^{r_i}\right).
\end{aligned}$$

Note that u/v is well defined here since $v = \Lambda_2 \not\equiv 0 \pmod{p}$. The conditions $\Lambda_1 \not\equiv 0 \pmod{p}$, $\Lambda_2 \not\equiv 0 \pmod{p}$ show that we may replace the summation by $\sum_{u=1}^{p-1} \sum_{v=1}^{p-1}$. We may ignore the restriction $\Lambda_i \not\equiv 0 \pmod{p}$, since if $\Lambda_j \equiv 0 \pmod{p}$ for some j then $\chi\left(\prod_{i=1}^{5} \Lambda_i^{r_i}\right) = 0$ and there is no contribution to the sum. Thus we take the sum over $1 \le u, v \le p-1$. The change of variables $v \to v$, $\frac{u}{v} \to \lambda$ is non-singular on $\mathbb{Z}_p^* \times \mathbb{Z}_p^*$, so

$$S_0 = \sum_{u=1}^{p-1} \sum_{v=1}^{p-1} \chi\left(v^{r_1+\cdots+r_5} \prod_{i=1}^{5} (a_i \frac{u}{v} + b_i)^{r_i}\right)$$

$$= \sum_{v=1}^{p-1}\sum_{\lambda=1}^{p-1}\chi\left(v^{r_1+\cdots+r_5}\prod_{i=1}^{5}(a_i\lambda+b_i)^{r_i}\right)$$
$$= \sum_{v=1}^{p-1}\chi\left(v^{r_1+\cdots+r_5}\right)\sum_{\lambda=1}^{p-1}\chi\left(\prod_{i=1}^{5}(a_i\lambda+b_i)^{r_i}\right). \qquad (4.12)$$

We now separate the two cases $r_1+\cdots+r_5 \not\equiv 0 \pmod{k}$ and $r_1+\cdots+r_5 \equiv 0 \pmod{k}$.

1. $R = r_1+\cdots+r_5 \not\equiv 0 \pmod{k}$. Since χ has order k, $\chi^R \neq \chi_0$. Hence,

$$\sum_{v=1}^{p-1}\chi\left(v^{r_1+\cdots+r_5}\right) = \sum_{v=1}^{p-1}\chi\left(v^R\right) = \sum_{v=1}^{p-1}\chi^R(v) = 0.$$

   Hence $S_0 = 0$ for these values of $r_1,\ldots,r_5$.

2. $R = r_1+\cdots+r_5 = kw$ for some w, and so $\chi\left(v^{r_1+\cdots+r_5}\right) = \chi\left(v^{kw}\right) = 1$, since χ has order k. Thus,

$$S_0 = (p-1)\sum_{\lambda=1}^{p-1}\chi\left(\prod_{i=1}^{5}(a_i\lambda+b_i)^{r_i}\right).$$

Now $a_2 \equiv 0 \pmod{p}$, and $b_2 \equiv 1 \pmod{p}$, so

$$\prod_{i=1}^{5}(a_i\lambda+b_i)^{r_i} = \prod_{i=1,i\neq 2}^{5}(a_i\lambda+b_i)^{r_i}.$$

Since $\rho = 1$, no other $a_i \equiv 0 \pmod{p}$ and we may apply Lemma 22 with $t = 4$ to give

$$S_0 \leq (p-1)(3\sqrt{p}+1).$$

We can now complete the evaluation of $|\Sigma_0|$:

$$\Sigma_0 = \sum_{\substack{r_1,\ldots,r_5\\ 1\leq r_i\leq k-1}} \tau\left(\overline{\chi}^{r_1}\right)\cdots\tau\left(\overline{\chi}^{r_5}\right)\left[\sum_{\substack{u,v\\ \Lambda_i\not\equiv 0\ (p)}}\chi\left(\Lambda_1^{r_1}\cdots\Lambda_5^{r_5}\right)\right]$$
$$= \sum_{\substack{r_1,\ldots,r_5\\ 1\leq r_i\leq k-1}} \tau\left(\overline{\chi}^{r_1}\right)\cdots\tau\left(\overline{\chi}^{r_5}\right) S_0$$

But for each set of values of $(r_1, \ldots, r_5)$, $|\tau(\overline{\chi}^{r_1}) \cdots \tau(\overline{\chi}^{r_5})| = p^{\frac{5}{2}}$ by (4.5). Now

$$\Sigma_0 = \sum_{r_1+\cdots+r_5=0\ (k)} \tau(\overline{\chi}^{r_1}) \cdots \tau(\overline{\chi}^{r_5})\, S_0 + \sum_{r_1+\cdots+r_5\neq 0\ (k)} \tau(\overline{\chi}^{r_1}) \cdots \tau(\overline{\chi}^{r_5})\, S_0$$

Hence,

$$\begin{aligned} |\Sigma_0| &\leq p^{\frac{5}{2}} \sum_{r_1+\cdots+r_5=0\ (k)} |S_0| + p^{\frac{5}{2}} \sum_{r_1+\cdots+r_5\neq 0\ (k)} |S_0|\,. \\ &= p^{\frac{5}{2}} \sum_{r_1+\cdots+r_5=0\ (k)} |S_0| \end{aligned}$$

It is easy to see that

$$\#\{r_1 + \cdots + r_5 \equiv 0 \pmod{k} : 1 \leq r_i \leq k-1\} \leq (k-1)^4.$$

Thus,

$$|\Sigma_0| \leq p^{\frac{5}{2}}(p-1)(3\sqrt{p}+1)(k-1)^4. \tag{4.13}$$

4.6 Estimate for Σ_1

First we assume that $u \equiv \Lambda_1 \equiv 0 \pmod{p}$. We need to estimate the contribution to the sum on the right hand side of (4.11) with $u \equiv 0 \pmod{p}$. This is done in the standard way, since $b_i \not\equiv 0 \pmod{p}$ for $2 \leq i \leq 5$.

$$\begin{aligned} \Sigma &= (p-1) \sum_{v=1}^{p-1} \prod_{i=2}^{5} T(b_i v) \\ &\leq (p-1) \sum_{v=1}^{p-1} |T(v)|^4 = (p-1) S_4 \end{aligned}$$

since $b_i \not\equiv 0 \pmod{p}$ for $2 \leq i \leq 5$. So, using (4.8),

$$\Sigma \leq (p-1)(k-1)^3 p^3 \leq p^4 (k-1)^3.$$

Now we need to multiply by 5 since any Λ_i could be zero (mod p). Thus we see that

$$|\Sigma_1| \leq 5p^4(k-1)^3. \tag{4.14}$$

We can now finish the case $\rho = 1$. From (4.11), (4.13) and (4.14),

$$\begin{aligned} \left|pN - p^5\right| &\leq |\Sigma_0| + |\Sigma_1| \\ &\leq p^{\frac{5}{2}}(p-1)(3\sqrt{p}+1)(k-1)^4 + 5p^4(k-1)^3. \end{aligned}$$

For $N > 0$ we need

$$p^{\frac{5}{2}}(p-1)(3\sqrt{p}+1)(k-1)^4 + 5p^4(k-1)^3 < p^5$$

or equivalently,

$$\left(\frac{p-1}{p}\right)\left(3 + \frac{1}{\sqrt{p}}\right)(k-1)^4 + 5(k-1)^3 < p.$$

Now, for $p > 3k^4$,

$$\begin{aligned} \left(3 + \frac{1}{\sqrt{p}}\right)(k-1)^4 &< 3(k-1)^4 + \frac{(k-1)^4}{\sqrt{3k^2}} \\ &< 3(k-1)^4 + k^2. \end{aligned}$$

Also, $\dfrac{p-1}{p} < 1$, so for $p > 3k^4$,

$$\begin{aligned} &\left(\frac{p-1}{p}\right)\left(3 + \frac{1}{\sqrt{p}}\right)(k-1)^4 + 5(k-1)^3 \\ < \;& 3(k-1)^4 + k^2 + 5(k-1)^3 \\ = \;& 3k^4 - 7k^3 + 4k^2 + 3k - 2 \\ < \;& 3k^4 < p. \end{aligned}$$

Thus we have a solution for all $p > 3k^4$.

4.7 Theorem 16: the case $\rho = 2$.

We begin by using elementary row operations to put the congruences in the form

$$\begin{aligned} f_0 &= x_1^k + a_2x_2^k + a_3x_3^k + \cdots + a_5x_5^k \equiv 0 \pmod{p} \\ g_0 &= \qquad\qquad b_3x_3^k + \cdots + b_5x_5^k \equiv 0 \pmod{p}, \end{aligned} \tag{4.15}$$

where possibly $a_4 \equiv 0 \pmod{p}$, $a_5 \not\equiv 0 \pmod{p}$ and $b_3b_4b_5 \not\equiv 0 \pmod{p}$.

Lemma 25 *Let $p \equiv 1 \pmod{k}$. If $r = 2$ then the congruences (4.15) have a solution of rank 2 (mod p), provided that $p > k^4$.*

Proof. We begin by solving

$$b_3x_3^k + \cdots + b_5x_5^k \equiv 0 \pmod{p}$$

with $x_3x_4x_5 \not\equiv 0 \pmod{p}$ using Lemma 24. This solution involves 2 linearly independent columns of coefficients.

Let $A = a_3x_3^k + a_4x_4^k + a_5x_5^k$. If $A \equiv 0 \pmod{p}$, take $x_1 = x_2 = 0$ to give the required solution. If $A \not\equiv 0 \pmod{p}$, multiply x_3, x_4, x_5 by ξ and solve

$$x_1^k + a_2x_2^k + A\xi^k \equiv 0 \pmod{p}$$

with $x_1x_2\xi \not\equiv 0 \pmod{p}$ using Lemma 7, which also gives us the required solution. ■

Thus we may now combine our two results for $\rho = 1$ and $\rho = 2$. We have shown that the congruences (4.2) have a solution of rank 2 (mod p) for all $p > 3k^4$. Hence by Lemma 18 the equations (4.1) have a non-trivial p-adic solution for all such p, and so Theorem 16 is proved.

4.8 Extensions to $r > 2$ equations

The same technique of counting numbers of solutions using multiplicative sums can also be used to solve $r > 2$ simultaneous equations. We can write

$$q^rN = \sum_{\mathbf{u} \in \mathbb{F}_q^r} T(\Lambda_1) \cdots T(\Lambda_{2r+1})$$

as before, and then use lemma 20 to introduce multiplicative characters. The only difficulty concerns values of the u for which certain Λ_i vanish and hence $T(\Lambda_i) = q$. These must be dealt with before using lemma 20, by partitioning the sum over the values of $\mathbf{u} \in \mathbb{F}_q^r$. The polynomial character sums arising can then be estimated using our main conjecture for the generalised Hasse-Weil character sum estimate. In fact, it turns out that the estimate for homogeneous polynomials that follows from this is more appropriate. We have not attempted to complete this calculation but believe that this is the most appropriate method for attacking these kind of problems for diagonal equations.

Chapter 5

Simultaneous Additive Equations

5.1 Introduction

We restate for convenience the result of Atkinson, Brüdern and Cook [4] for systems of additive equations over the field of p-adic numbers:

Theorem (Atkinson Brüdern and Cook)
Let r, k, n be positive integers with $k > 1$ and $n > 2rk$. Then the system of equations

$$F_i(x) = a_{i1}x_1^k + \cdots + a_{in}x_n^k = 0, \qquad i = 1, ..., r \tag{5.1}$$

with coefficients $a_{ij} \in \mathbb{Z}$, has a non-trivial p-adic solution for all $p > k^{2r+2}$.

In this chapter the same problem is considered for equations in $n > crk$ variables where c is a positive integer and $c \geq 3$. A similar approach to that of the above authors is adopted, differing mainly in the exponential sum arguments, and the handling of singular solutions.

Theorem 26 *Let r, k, n, c be positive integers with $k > 1$, $n > crk$ and $c > 2$. Then the system of equations (5.1), with coefficients $a_{ij} \in \mathbb{Z}$, has a non-trivial p-adic solution for all $p > r^2k^{2+\frac{2}{c-2}}$ if $r \neq 1$, and $p > k^{2+\frac{2}{c-1}}$ if $r = 1$.*

As usual, p-adic solutions are obtained by a Hensel's Lemma argument from non-singular solutions to certain congruences. However, the congruences (mod p) are solved by an induction

argument on r. In our proof, as in [4], not only homogenous congruences, but also inhomogeneous congruences must be considered. This auxiliary result on congruences may be of independent interest so it is described in detail.

5.2 Preliminaries to Theorem 26

Let $B = (b_{ij})$ be an $r \times m$ matrix over the field $\mathbf{K}$. For $0 \leq d \leq r$ we denote by $\mu(d, B)$ the maximum number of columns from B which can lie in a d-dimensional subspace of $\mathbf{K}^r$. In particular, if $m = cr + 1$ and $\mu(d, B) \leq cd$ holds for all $d \leq r - 1$, then we call B *highly non-singular.*

For b_{ij}, $d_i \in \mathbb{Z}$, a solution $\mathbf{x}$ to the congruences

$$b_{i1}x_1^k + \cdots + b_{im}x_m^k \equiv d_i \pmod{p}, \quad i = 1, \ldots, r \tag{5.2}$$

is said to be of rank ρ if the matrix $(b_{ij}x_j)$ has rank ρ in $\mathbb{F}_p$, and is non-singular if it has maximal rank.

Theorem 27 *Let $m = cr + 1$, b_{ij}, $d_i \in \mathbb{Z}$ be such that $B = (b_{ij})$ is highly non-singular in the field $\mathbf{F_p}$. Then the system of congruences (5.2), mod p, has a non-singular solution mod p for all primes $p > r^2k^{2+\frac{2}{c-2}}$ if $r \neq 1$, and $p > k^{2+\frac{2}{c-1}}$ if $r = 1$.*

We shall only require Theorem 27 in the case $\mathbf{K} = \mathbb{F}_p$ for the proof of Theorem 26; however the result also holds in the more general setting of a finite field $\mathbf{K} = \mathbb{F}_q$ $\left(q = p^f\right)$ and we outline this generalisation in Section 5.6.

5.3 Proof of Theorem 27

Lemma 28 (Aigner) *Let A be an $r \times m$ matrix over a field $\mathbf{K}$ and let t be a positive integer. Then A includes t disjoint $r \times r$ submatrices which are non-singular over $\mathbf{K}$ if and only if*

$$m - \mu(d, A) \geq t(r - d) \tag{5.3}$$

holds for all $d \leq r - 1$.

Corollary 29 *If A contains a set $\mathbf{T}$ of c independent columns, then we can choose the t disjoint submatrices to include these.*

Aigner [1] gives a proof of the lemma.

Proof of corollary

Let us assume that at least one of the c columns cannot be included in the t disjoint submatrices. Then there must be a smallest set $\mathbf{S}$ of excluded columns. Choose an element $\mathbf{v}$ from this set and one of the submatrices, $\mathbf{R}$. Then since $\mathbf{R}$ is non-singular, it has rank r and $\mathbf{v}$ may be expressed as a non-zero combination of certain columns in $\mathbf{R}$. Also these columns cannot all be in $\mathbf{T}$ since $\mathbf{T}$ is an independent set. Exchanging $\mathbf{v}$ with one of these columns not in $\mathbf{T}$ still gives a matrix $\mathbf{R}'$ of rank r, and a smaller set $\mathbf{S}' = \mathbf{S} \backslash \{\mathbf{v}\}$. Thus, we have a contradiction to the assumption of a smallest set. Hence our initial assumption is false and the corollary holds. ■

It follows immediately from the lemma that if $\mathbf{B}$ is an $r \times (cr + 1)$ highly non-singular matrix, then $\mathbf{B}$ contains c $r \times r$ non-singular matrices. Renumbering the variables and using row operations, the matrix of coefficients $\mathbf{B}$ in the congruences (27) may be brought to the shape $\mathbf{B} = [\mathbf{I}, \mathbf{B}_0]$ where $\mathbf{I}$ is the $r \times r$ identity matrix and $\mathbf{B}_0$ is $r \times ((c-1)r + 1)$. With this

matrix of coefficients and $\mathbf{u} = (u_1, \ldots, u_r)$ we associate linear forms

$$\Lambda_j = u_1 b_{1j} + \cdots + u_r b_{rj} \ , \ j = 1, \ldots, m, \tag{5.4}$$

where $m = cr + 1$. Then

$$\Lambda_j = u_j \text{ for } j = 1, \ldots, r. \tag{5.5}$$

For $1 \leq v \leq r$ we define $q_v(\mathbf{B})$ as the minimal number of components with a non-zero entry in at least one out of any v linearly independent linear combinations of the rows of $\mathbf{B}$. Then for any $r \times m$ matrix $\mathbf{B}$ we have

$$\mu(d, \mathbf{B}) + q_{r-d}(\mathbf{B}) = m. \tag{5.6}$$

Note that the $r \times (cr + 1)$ matrix $\mathbf{B}$ is highly non-singular, if and only if, $q_i(\mathbf{B}) > ci$ for $i = 0, \ldots, r - 1$.

We classify the points $\mathbf{u} \neq 0$ into subsets $\wp_\tau$ $(\tau = 0, \ldots r-1)$ where $u_{\tau+1}$ is the first non-zero variable amongst the $u_1, \ldots u_r$. Thus

$$\wp_\tau = \left\{ \mathbf{u} \in \mathbb{F}_p^r : u_1 = \cdots = u_\tau = 0, \ u_{\tau+1} \neq 0 \right\}, \ 0 \leq \tau \leq r - 1. \tag{5.7}$$

For a fixed τ with $0 \leq \tau \leq r - 1$, let Λ_j' $(j = 1, \ldots, m)$ denote the restrictions of the forms Λ_j to the vector space $\wp_\tau' = \wp_\tau \cup \{0\}$. In this subspace the forms $\Lambda_1', \ldots, \Lambda_m'$ have an $(r - \tau) \times m$ matrix

$$\mathbf{B}' = [\mathbf{0}_\tau, \mathbf{I}_{r-\tau}, \mathbf{B}_1],$$

where $\mathbf{B}_1$ consists of the last $r - \tau$ rows of $\mathbf{B}_0$. If we take any v independent linear combinations of the rows of $\mathbf{B}'$, then we are simply taking the same independent linear combinations of the rows of $\mathbf{B}$, so $q_v\left(\mathbf{B}'\right) \geq q_v\left(\mathbf{B}\right)$ for $v = 1, \ldots r - \tau$. Thus,

$$q_v\left(\mathbf{B}'\right) > cv \text{ for } v = 1, \ldots, r - \tau - 1.$$

The first non-zero column corresponds to $u_{\tau+1}$ and the remaining $cr - \tau$ columns give an $(r - \tau) \times (cr - \tau)$ matrix $\mathbf{B}''$ satisfying $q_v\left(\mathbf{B}''\right) \geq cv$. Therefore, by Aigner's criterion, these $cr - \tau$ columns will contain c disjoint non-singular $(r - \tau) \times (cr - \tau)$ matrices which we can

arrange to contain the columns corresponding to $u_{\tau+1},\ldots,u_r$ by corollary (29). We can now renumber columns $\tau+2,\ldots cr+1$ to give c disjoint sets of $r-\tau$ elements

$$V_i = \{(i-1)r-(i-2)\tau+2,\ldots,ir-(i-1)\tau+1\}, \qquad i=1,\ldots,c \tag{5.8}$$

such that for $i=1,\ldots,c$ the restrictions Λ_v^* to $\wp_\tau$ of the linear forms Λ_v, $v\in V_i$, are sets of linearly independent forms.

Theorem 27 will now be proved by counting the number of solutions to (5.2) with the first r variables non-zero. Since the corresponding forms Λ_i, $i=1,\ldots,r$ form a matrix of rank r ($\mathbf{I}_{r\times r}$), this automatically guarantees a non-singular solution. The solutions are counted using exponential sums,

$$T^*(u) = \sum_{x=1}^{p-1} e\left(\frac{ux^k}{p}\right) \tag{5.9}$$

$$T(u) = \sum_{x=1}^{p} e\left(\frac{ux^k}{p}\right) \tag{5.10}$$

For $u\not\equiv 0 \pmod p$ we have, from Lemma 12 of Davenport [22],

$$|T^*(u)| \le (k-1)\sqrt{p}+1 < k\sqrt{p} \tag{5.11}$$

$$|T(u)| \le (k-1)\sqrt{p} < k\sqrt{p} \tag{5.12}$$

Let

$$S_c = \sum_{u=1}^{p} |T(u)|^c, \quad S_c^* = \sum_{u=1}^{p} |T^*(u)|^c. \tag{5.13}$$

Lemma 30 *We have*

$$\begin{gathered} p^c < S_c \le (p-1)p^{\frac{c}{2}}k^{c-1}+p^c \\ (p-1)^c < S_c^* \le (p-1)p^{\frac{c}{2}}k^{c-1}+(p-1)^c. \end{gathered} \tag{5.14}$$

Proof. Let $\Upsilon_c = \sum_{u=1}^{p-1}|T(u)|^c$. This is the same as S_c but summing from 1 to $p-1$ instead of p. Now $p^{-1}S_2$ equals the number of solutions to the congruence $x^k \equiv y^k \pmod p$. For each

$x \neq 0 \pmod{p}$ there are k solutions for y so

$$S_2 = p((p-1)k+1).$$

Since $\Upsilon_2 = S_2 - p^2$ we have

$$\begin{aligned} \Upsilon_2 = p((p-1)k+1) - p^2 &= (k-1)p(p-1) \\ &< kp(p-1). \end{aligned}$$

Similarly on defining $\Upsilon_c^* = \sum_{u=1}^{p-1} |T^*(u)|^c$ we have

$$\Upsilon_2^* = p((p-1)k) - (p-1)^2 < kp(p-1).$$

Hence using (5.11) we find

$$\begin{aligned} 0 < \Upsilon_c = \sum_{u=1}^{p-1} |T(u)|^c < \Upsilon_2 (k\sqrt{p})^{c-2} < (p-1)p^{\frac{c}{2}} k^{c-1} \\ 0 < \Upsilon_c^* = \sum_{u=1}^{p-1} |T^*(u)|^c < \Upsilon_2^* (k\sqrt{p})^{c-2} < (p-1)p^{\frac{c}{2}} k^{c-1}, \end{aligned} \tag{5.15}$$

and finally using the formulas

$$\begin{aligned} S_c &= \Upsilon_c + p^c \\ S_c^* &= \Upsilon_c^* + (p-1)^c, \end{aligned}$$

we obtain (5.14). ■

We first consider the case $r = 1$. Then any non-trivial solution is non-singular. Hence the number N of non-singular solutions to (5.2) is given by

$$pN = \sum_{u_1 \pmod{p}} T^*(b_{11}u_1)T(b_{12}u_1)\cdots T(b_{1c+1}u_1)e\left(-\frac{u_1 d_1}{p}\right).$$

Separating out the term $u_1 = 0$, taking the modulus of both sides and applying the triangle

inequality we have,

$$|pN-(p-1)p^c| \leq \sum_{u_1\not\equiv 0 \pmod p} |T^*(b_{11}u_1)T(b_{12}u_1)\cdots T(b_{1c+1}u_1)| \tag{5.16}$$

$$= \sum_{u_1=1}^{p-1} |T^*(b_{11}u_1)T(b_{12}u_1)\cdots T(b_{1c+1}u_1)| \tag{5.17}$$

$$\leq \left\{ \sum_{u_1=1}^{p-1} |T^*(b_{11}u_1)|^{c+1} \sum_{u_1=1}^{p-1} |T(b_{12}u_1)|^{c+1} \cdots \sum_{u_1=1}^{p-1} |T(b_{1c+1}u_1)|^{c+1} \right\}^{\frac{1}{c+1}} \tag{5.18}$$

As u runs through $1,\ldots,p-1$ so does $(b_{1i}u_1)$, $i=1,\ldots,m$. Thus (5.18) implies

$$\begin{aligned} |pN-(p-1)p^c| &\leq \Upsilon_{c+1}^{*\frac{1}{c+1}} \Upsilon_{c+1}^{\frac{c}{c+1}} \\ &\leq (p-1)p^{\frac{c+1}{2}}k^c. \end{aligned}$$

by 5.15. Thus for $N>0$ we require

$$(p-1)p^{\frac{c+1}{2}}k^c < (p-1)p^c,$$

which is equivalent to $p > k^{2+\frac{2}{c-1}}$.

Now if $r>1$, then the number N of incongruent solutions to the r congruences (5.2) with the first r variables non-zero is given by

$$p^rN = \sum_{\mathbf{u} \bmod p} T^*(\Lambda_1)\cdots T^*(\Lambda_r)T(\Lambda_{r+1})\cdots T(\Lambda_m)e\left(-\frac{\mathbf{u}\cdot\mathbf{d}}{p}\right). \tag{5.19}$$

Separating out the term $\mathbf{u}\equiv 0$, taking the modulus of both sides we have

$$p^rN-(p-1)^rp^{m-r} \leq \sum_{\mathbf{u}\not\equiv \mathbf{0} \bmod p} |T^*(\Lambda_1)\cdots T^*(\Lambda_r)T(\Lambda_{r+1})\cdots T(\Lambda_m)|. \tag{5.20}$$

We classify the points $\mathbf{u}\not\equiv 0$ into the subsets $\wp_\tau$, $\tau=0,\ldots,r-1$, and let Σ_τ denote the contribution to the right-hand side of (5.20) coming from the points $\mathbf{u}\in\wp_\tau$. Then

$$|p^rN-(p-1)^rp^{m-r}| \leq \Sigma_0+\cdots+\Sigma_{r-1},$$

and using the trivial estimate for $|T^*(u)|$,

$$\Sigma_\tau \leq (p-1)^\tau \sum_{\mathbf{u}\in\wp_\tau} |T^*(\Lambda_{\tau+1})\cdots T^*(\Lambda_r)T(\Lambda_{r+1})\cdots T(\Lambda_m)|\,.$$

Further, on $\wp_\tau$ we have $u_{\tau+1} \neq 0 \bmod p$ and so, from (5.11)

$$|T^*(u_{\tau+1})| = |T^*(\Lambda_{\tau+1})| \leq (k-1)\sqrt{p}+1. \tag{5.21}$$

For $i = 1,\ldots,c$ the mappings $(u_{\tau+1},\ldots,u_r) \longmapsto (\Lambda'_v : v \in V_i)$, where V_i is defined in (5.8), are non-singular. We now define Θ_i, $1 \leq i \leq c$, where α_i of the $\mathbf{T}$'s are T and β_i of the $\mathbf{T}$'s are T^*.

$$\Theta_i = \sum_{\wp_\tau} \prod_{v\in V_i} \left|\mathbf{T}(\Lambda'_v)\right|^c = \sum_{\wp_\tau} \prod_{j=\tau+1}^{r} |\mathbf{T}(u_j)|^c = S_c^{\alpha_i} S_c^{*\beta_i} \tag{5.22}$$

Since the columns in $V_1,\ldots,V_c$ contain exactly $r-t-1$ with T^*, and $(c-1)(r-\tau)+1$ with T we have

$$\begin{aligned} \sum_{i=1}^{c} \alpha_i &= (c-1)(r-\tau)+1 \\ \sum_{i=1}^{c} \beta_i &= r-t-1. \end{aligned}$$

Hence,

$$\Theta_1\cdots\Theta_c = \prod_{i=1}^{c} S_c^{\alpha_i} S_c^{*\beta_i} = S_c^{\left[\sum_{i=1}^c \alpha_i\right]} S_c^{*\left[\sum_{i=1}^c \beta_i\right]} \tag{5.23}$$

$$= S_c^{(c-1)(r-\tau)+1} S_c^{*(r-t-1)}. \tag{5.24}$$

The estimation of Σ_τ is now easily completed. For $T^*(u_{\tau+1})$ we have the estimate (5.21), and for all other $T(\Lambda_v)$ with v in none of the $V_1,\ldots,V_c$ we use the trivial bound. Thus, by an extension of Hölder's inequality (see [38], theorem 11, p.22)

$$\begin{aligned} \Sigma_\tau &\leq ((k-1)\sqrt{p}+1)\, p^{(c-1)\tau}(p-1)^\tau (\Theta_1\cdots\Theta_c)^{\frac{1}{c}} \\ &\leq ((k-1)\sqrt{p}+1)\, p^{(c-1)\tau}(p-1)^\tau \left(S_c^{(c-1)(r-\tau)+1} S^{*(r-t-1)}\right)^{\frac{1}{c}}. \end{aligned} \tag{5.25}$$

From (5.20) we now have

$$|p^r N - (p-1)^r p^{m-r}| \leq ((k-1)\sqrt{p}+1)\, S_c^{\frac{r(c-1)+1}{c}} S_c^{*\frac{r-1}{c}} \sum_{\tau=0}^{r-1} \left(\frac{p^{c-1}(p-1)}{S_c^{\frac{c-1}{c}} S_c^{*\frac{1}{c}}} \right)^{\tau}. \tag{5.26}$$

From (5.14), we have $S_c^* > (p-1)^c$ and $S_c > p^c$, so (5.26) becomes

$$\begin{aligned} |p^r N - (p-1)^r p^{m-r}| &\leq ((k-1)\sqrt{p}+1)\, r S_c^{\frac{r(c-1)+1}{c}} S_c^{*\frac{r-1}{c}} \qquad (5.27) \\ &\leq ((k-1)\sqrt{p}+1)\, r \left(p^{\frac{c}{2}}(p-1)k^{c-1} + (p-1)^c \right)^{\frac{r-1}{c}} \left(p^{\frac{c}{2}}(p-1)k^{c-1} + p^c \right)^{\frac{r(c-1)+1}{c}}, \end{aligned}$$

using (5.14). Thus we see that for $N > 0$, we require

$$\begin{aligned} & r((k-1)\sqrt{p}+1) \left(p^{\frac{c}{2}}(p-1)k^{c-1} + (p-1)^c \right)^{\frac{r-1}{c}} \left(p^{\frac{c}{2}}(p-1)k^{c-1} + p^c \right)^{\frac{r(c-1)+1}{c}} \\ < \;& (p-1)^r p^{(c-1)r+1}. \end{aligned} \tag{5.28}$$

Dividing through by $(p-1)^{r-1}p^{(c-1)r+1\frac{1}{2}}$, this is equivalent to

$$\begin{aligned} & r\left(k-1+\frac{1}{\sqrt{p}}\right) \left(\frac{p^{\frac{c}{2}}k^{c-1}}{(p-1)^{c-1}} + 1 \right)^{\frac{r-1}{c}} \left(\frac{(p-1)k^{c-1}}{p^{\frac{c}{2}}} + 1 \right)^{\frac{r(c-1)+1}{c}} \\ < \;& \sqrt{p}\left(1-\frac{1}{p}\right). \end{aligned} \tag{5.29}$$

This inequality is difficult to work with, so we replace it by

$$r\left(k-1+\frac{1}{\sqrt{p}}\right) \left(\frac{p^{\frac{c}{2}}k^{c-1}}{(p-1)^{c-1}} + 1 \right)^{\frac{r}{c}} \left(\frac{(p-1)k^{c-1}}{p^{\frac{c}{2}}} + 1 \right)^{\frac{r(c-1)}{c}} < \nu(k)\sqrt{p} \tag{5.30}$$

where $\nu(k) = \left(1 - 1/k^{2+\frac{2}{c-2}}\right)$ which implies (5.29) because

$$\frac{p^{\frac{c}{2}}k^{c-1}}{(p-1)^{c-1}} + 1 > \frac{(p-1)k^{c-1}}{p^{\frac{c}{2}}} + 1$$

and $p > r^2 k^{2+\frac{2}{c-2}}$.

We now assume $p > r^2 k^{2+\frac{2}{c-2}}$ and show that it leads to (5.30).

First, $p > r^2 k^{2+\frac{2}{c-2}}$ implies $\frac{k^{c-1}}{p^{\frac{c}{2}-1}} < \frac{1}{r^{c-2}}$. Thus

$$\frac{(p-1)k^{c-1}}{p^{\frac{c}{2}}} + 1 < \frac{1}{r^{c-2}} + 1$$

and

$$\begin{aligned} \frac{p^{\frac{c}{2}}k^{c-1}}{(p-1)^{c-1}} + 1 &= \left(\frac{p}{p-1}\right)^{c-1} \frac{k^{c-1}}{p^{\frac{c}{2}-1}} + 1 \\ &< \left(\frac{p}{p-1}\right)^{c-1} \frac{1}{r^{c-2}} + 1. \end{aligned}$$

Hence,

$$\begin{aligned} & r\left(k-1+\frac{1}{\sqrt{p}}\right)\left(\frac{p^{\frac{c}{2}}k^{c-1}}{(p-1)^{c-1}}+1\right)^{\frac{r}{c}}\left(\frac{(p-1)k^{c-1}}{p^{\frac{c}{2}}}+1\right)^{\frac{r(c-1)}{c}} \\ < \; & r\left(k-1+\frac{1}{\sqrt{p}}\right)\left(\left(\frac{p}{p-1}\right)^{c-1}\frac{1}{r^{c-2}}+1\right)^{\frac{r}{c}}\left(\frac{1}{r^{c-2}}+1\right)^{\frac{r(c-1)}{c}}. \end{aligned} \tag{5.31}$$

By the exponential inequality

$$\left(1+\frac{x}{n}\right)^n < \exp(x),$$

we have

$$\begin{aligned} \left(\left(\frac{p}{p-1}\right)^{c-1}\frac{1}{r^{c-2}}+1\right)^{\frac{r}{c}} &< \exp\left(\left(\frac{p}{p-1}\right)^{c-1}\frac{1}{cr^{c-3}}\right) \\ \text{and} \quad \left(\frac{1}{r^{c-2}}+1\right)^{r\frac{c-1}{c}} &< \exp\left(\frac{c-1}{cr^{c-3}}\right). \end{aligned}$$

Thus

$$\begin{aligned} & r\left(k-1+\frac{1}{\sqrt{p}}\right)\left(\left(\frac{p}{p-1}\right)^{c-1}\frac{1}{r^{c-2}}+1\right)^{\frac{r}{c}}\left(\frac{1}{r^{c-2}}+1\right)^{r\frac{c-1}{c}} \\ < \; & r\left(k-1+\frac{1}{\sqrt{p}}\right)\exp\left(\left(\frac{p}{p-1}\right)^{c-1}\frac{1}{cr^{c-3}}+\frac{c-1}{cr^{c-3}}\right). \end{aligned}$$

So, for (5.30) to hold we need

$$\begin{aligned} r\left(k-1+\frac{1}{\sqrt{p}}\right)\exp\left(\left(\frac{p}{p-1}\right)^{c-1}\frac{1}{cr^{c-3}}+\frac{c-1}{cr^{c-3}}\right) &< \nu(k)rk^{1+\frac{1}{c-2}} \\ \Leftrightarrow \exp\left(\left(\frac{p}{p-1}\right)^{c-1}\frac{1}{cr^{c-3}}+\frac{c-1}{cr^{c-3}}\right) &< \frac{\nu(k)kk^{\frac{1}{c-2}}}{k-1+\frac{1}{\sqrt{p}}} \\ \Leftrightarrow \exp\left(\frac{c-2}{cr^{c-3}}\left(\left(\frac{p}{p-1}\right)^{c-1}+c-1\right)\right) &< k\left(\frac{\nu(k)k}{k-1+\frac{1}{\sqrt{p}}}\right)^{c-2}. \end{aligned} \tag{5.32}$$

Now,

$$\frac{p}{p-1}=\frac{1}{1-\frac{1}{p}}<\frac{1}{1-\frac{1}{16}}=\frac{16}{15}$$

since $p > r^2k^2 \geq 16$. This gives us

$$\exp\left(\frac{c-2}{cr^{c-3}}\left(\left(\frac{p}{p-1}\right)^{c-1}+c-1\right)\right)<\exp\left(\frac{c-2}{cr^{c-3}}\left(\left(\frac{16}{15}\right)^{c-1}+c-1\right)\right). \tag{5.33}$$

Let us denote the RHS of (5.33) by $f(c,r)$. Then we have

$$f(c,r) = \exp\left(\frac{c-2}{cr^{c-3}}\left(\left(\frac{16}{15}\right)^{c-1}+c-1\right)\right) \tag{5.34}$$

$$= \exp\left(\frac{r^2(c-2)}{c}\left(\left(\frac{16}{15r}\right)^{c-1}+\frac{c-1}{r^{c-1}}\right)\right). \tag{5.35}$$

From (5.34) f is a decreasing function in r, and from (5.35) f is a decreasing function in c. Therefore to find an upper bound on f we just evaluate $f(3,2) = 2.846...$

If $c \geq 4$ then

$$\begin{aligned} k\left(\frac{\nu(k)k}{k-1+\frac{1}{\sqrt{p}}}\right)^{c-2} &> k\left(\frac{k+1}{k}\frac{k-1}{k-1+\frac{1}{2k}}\right)^{c-2} \\ &= k\left(\frac{k^2-1}{k^2-k+\frac{1}{2}}\right)^{c-2} \\ &\geq 2\left(\frac{3}{2\frac{1}{2}}\right)^2=2.88 \end{aligned}$$

because $\nu(k) > (1-1/k^2)$, $p > 4k^2$ and $k \geq 2$. Hence in this case $f(3,2) = 2.846... < 2.88 <$

right hand side of (5.32). Thus (5.32) holds and we have a solution for all $c \geq 4$.

If $c = 3$ and $k = 2$,

$$\begin{aligned} k\left(\frac{\nu(k)k}{k-1+\frac{1}{\sqrt{p}}}\right)^{c-2} &= \frac{\nu(k)k^2}{k-1+\frac{1}{\sqrt{p}}} \\ &> \frac{\nu(k)2^2}{2-1+\frac{1}{4}} \\ &\geq \left(1-\frac{1}{16}\right)\frac{16}{5} = 3 \end{aligned}$$

because $\nu(k) = 1 - 1/k^4 \geq 1 - 1/16$ and $p > 16$. Hence, here also $f(3,2) = 2.846... < 3 <$ RHS of (5.32).

If $c = 3$ and $k > 2$,

$$\begin{aligned} k\left(\frac{\nu(k)k}{k-1+\frac{1}{\sqrt{p}}}\right)^{c-2} &= \frac{\nu(k)k^2}{k-1+\frac{1}{\sqrt{p}}} \\ &= \frac{\nu(k)k}{1-\frac{1}{k}+\frac{1}{k\sqrt{p}}} \\ &> \frac{3\times\frac{15}{16}}{1+\frac{1}{3\times 16}} = 3.85714 \end{aligned}$$

because $\nu(k) = 1 - 1/k^4 \geq 1 - 1/16$ and $p > 16$. Hence, here also $f(3,2) = 2.846... < 3.8 <$ RHS of (5.32).and we have a solution for all $c > 2$.

5.4 p-adic normalization

We recall the basic results of the p-adic normalization introduced by Davenport and Lewis [25], but refer to [25] for the details. With the forms $\mathbf{F}_1, \ldots, \mathbf{F}_r$ we associate the parameter

$$\theta = \prod_{\mathbf{J}} \det \mathbf{A}_J,$$

where $\mathbf{A}_J = (a_{ij})$, $1 \leq i \leq r$, $j \in \mathbf{J}$, is an $r \times r$ submatrix of $\mathbf{A}$ and $\mathbf{J}$ runs over all r-element subsets of $\{1, 2, \ldots, n\}$. By the arguments of §4 of Davenport and Lewis [25] it suffices to prove Theorem 26 for systems of forms with $\theta \neq 0$. Moreover, for fixed p, the equations (5.1) have a

non-trivial solution, if and only if, a related p-normalized system does. Further, p-normalized systems have the following properties.

Lemma 31 *Suppose that* $\mathbf{F}_1, \ldots, \mathbf{F}_r$ *is a* p*-normalized system, with* $\theta \neq 0$. *Then we may write (after renumbering the variables)*

$$\mathbf{F}_\ell = \mathbf{F}_{\ell,0} + p\mathbf{F}_{\ell,1}, \ 1 \leq \ell \leq r,$$

where

$$\mathbf{F}_{\ell,0} = \alpha_{\ell 1} x_1^k + \cdots + \alpha_{\ell m} x_m^k, \tag{5.36}$$

$\alpha_{ij} \in \mathbb{Z}$ *and each of* $x_1, \ldots, x_m$ *occurs in at least one of* $\mathbf{F}_{1,0}, \ldots, \mathbf{F}_{r,0}$ *with a coefficient not divisible by* p. *Also*

$$m \geq \frac{n}{k}. \tag{5.37}$$

Further, if we form any v *linear combinations of the* $\mathbf{F}_{\ell,0}$ *which are independent* mod p, *and denote by* q_v *the number of variables which occur in at least one of these combinations with a coefficient not divisible by* p, *then*

$$q_v \geq \frac{vn}{rk}, \ 1 \leq v \leq r-1. \tag{5.38}$$

This is lemma 11 of Davenport and Lewis [25]. The numbers q_v defined in this way correspond to the invariants $q_v(A) = q_v$ defined in section 2. We note that for $n > crk$ the inequalities (5.37) and (5.38) give

$$m > cr, \text{ and } q_v > cv, \text{ for } 1 \leq v \leq r-1 \tag{5.39}$$

Lemma 32 *If* p *does not divide* k *and the congruences*

$$\alpha_{\ell 1} x_1^k + \cdots + \alpha_{\ell m} x_m^k \equiv 0 \mod p, \qquad \ell = 1, \ldots, r$$

have a solution of rank $r \pmod p$, *then the equations*

$$\alpha_{\ell 1} x_1^k + \cdots + \alpha_{\ell m} x_m^k = 0$$

have a non-trivial p-adic solution.

This version of Hensel's Lemma is a particular case of Lemma 9 of Davenport and Lewis [25].

Now for $p > r^2k^{2+\frac{2}{c-2}}$ or $p > k^{2+\frac{2}{c-1}}$, we always have $p \nmid k$ so Theorem 26 follows from the following:

Proposition 33 *Let $\mathbf{F}_{\ell,0}$ be given by (5.36) and suppose that (5.39) holds. Then, for all $d_1, \ldots, d_r \in \mathbb{Z}$ and primes p satisfying $p > r^2k^{2+\frac{2}{c-2}}$ if $r \neq 1$, $p > k^{2+\frac{2}{c-1}}$ if $r = 1$, the congruences*

$$F_{\ell,0} \equiv d_\ell \mod p, \qquad 1 \leq \ell \leq r,$$

have a solution of rank r (mod p).

5.5 An inductive strategy

We prove the Proposition by induction on r. We recall (5.6) and (5.39), then writing $\mu(d)$ for $\mu(d, \mathbf{A})$, we have

$$\mu(d) < cd + m - cr \tag{5.40}$$

When $r = 1$ the Proposition is an immediate consequence of Theorem 27. We now suppose that the Proposition holds for systems with fewer than r congruences. If $m = cr + 1$, then (5.40) becomes $\mu(d) \leq cd$, so $\mathbf{A} = (\alpha_{ij})$ is highly non-singular and the Proposition follows from theorem 27.

We may now suppose that $m > cr + 1$. I shall show that either we can discard a column of $\mathbf{A}$ (that is, set the corresponding column to zero) and still satisfy (5.40) but with m replaced by $m - 1$; or we can solve the congruences by appealing to the induction hypothesis. This will prove the proposition, since after a finite number of steps either we reach the case $m = cr + 1$ (when there is a solution) or we obtain a solution by the induction hypothesis.

First we suppose that

$$\mu(d) < cd + m - cr - 1 \tag{5.41}$$

holds for all d with $1 \leq d \leq r - 1$. Then we may discard any column and still have (5.40) (with

m replaced by $m-1$).

Now we may suppose that for some d with $1 \leq d \leq r-1$ we have $\mu(d) = cd + m - cr - 1$. Then for $v = r - d$ we have

$$q_v = cv + 1 \tag{5.42}$$

where $q_v = q_v(\mathbf{A})$ and $\mathbf{A}$ is the matrix of coefficients in (5.39). Let t be the largest value of v for which (5.42) holds and put $d = r - t$. Applying row operations and relabelling, the system of congruences is equivalent to a system

$$\begin{array}{rcl}
b_{11}x_1^k + & \cdots & + b_{1m}x_1^k \equiv e_1 \\
\vdots & & \vdots \\
b_{d1}x_1^k + & \cdots & + b_{dm}x_1^k \equiv e_d \\
b_{d+1\eta}x_\eta^k + & \cdots & + b_{d+1m}x_m^k \equiv e_{d+1} \\
\vdots & & \vdots \\
b_{r\eta}x_\eta^k + & \cdots & + b_{rm}x_m^k \equiv e_r
\end{array}$$

where $\eta = m - ct$.

The last $r-d$ congruences contain $c(r-d)+1$ variables and this subsystem is highly non-singular (since we still have $q_i > ci$ in the subsystem). Thus by Theorem 27 the subsystem has a solution $\xi_\eta, \ldots, \xi_m$ of rank t. The system of congruences now becomes

$$\begin{array}{c}
b_{11}x_1^k + \cdots + b_{1\eta-1}x_{\eta-1}^k \equiv f_1 \\
\vdots \\
b_{d1}x_1^k + \cdots + b_{d\eta-1}x_{\eta-1}^k \equiv f_d
\end{array} \tag{5.43}$$

This subsystem contains

$$\eta - 1 = m - c(r-d) - 1 > cd \tag{5.44}$$

variables. Suppose that some v linear combinations have $q_v^* \leq cv$. Adjoining the last $r-d$ forms to those linear combinations we have $t+v$ independent linear combinations in at most $ct+1+cv$ variables, contrary to t being the largest value for which (5.42) holds. Therefore the subsystem (5.43) satisfies the conditions (5.39) of the Proposition, so by the induction hypothesis there is a solution of rank d. Combining this with $\xi_\eta, \ldots, \xi_m$ the whole system has a non-singular

solution, which completes the proof of Theorem 26.

5.6 Finite fields

Now $\mathbf{K} = \mathbb{F}_q$, where $q = p^f$,and $\mathbf{B} = (b_{ij})$ is highly non-singular over $\mathbf{K}$. We recall from Lemma 2D of Schmidt [54, p. 43] that all additive characters on $\mathbb{F}_q$ are given by

$$\Psi_u(x) = e\left(\frac{tr(ux)}{p}\right),$$

where $u \in \mathbb{F}_q$ and tr denotes the trace. We can now redefine T, T^*, S_c, S_c^* as

$$T^*(u) = \sum_{x \in \mathbb{F}_q} e\left(\frac{tr(ux^k)}{p}\right) \tag{5.45}$$

$$T(u) = \sum_{x \in \mathbb{F}_q^*} e\left(\frac{tr(ux^k)}{p}\right) \tag{5.46}$$

and

$$S_c = \sum_{u \in \mathbb{F}_q} |T(u)|^c \ , \ S_c^* = \sum_{u \in \mathbb{F}_q} |T^*(u)|^c . \tag{5.47}$$

If N now denotes the number of solutions of the system of equations

$$b_{i1}x_1^k + \cdots + b_{im}^k = d_i, \qquad i = 1, \ldots, r, \tag{5.48}$$

with $d_i \in \mathbb{F}_q$, then

$$q^r N = \sum_{\mathbf{u} \in \mathbf{F}_q^r} T^*(\Lambda_1) \cdots T^*(\Lambda_r) T(\Lambda_{r+1}) \cdots T(\Lambda_m) e\left(-\frac{tr(\mathbf{u} \cdot \mathbf{d})}{p}\right). \tag{5.49}$$

The analogues of (5.11) and (5.12) follow from Theorem 3D of Schmidt [54, p. 49] giving us

$$|T^*(u)| \leq (k-1)\sqrt{q} + 1 < k\sqrt{q} \tag{5.50}$$

and

$$|T(u)| \leq (k-1)\sqrt{q} < k\sqrt{q}. \tag{5.51}$$

Now $q^{-1}S_2$ equals the number of solutions of $x^k = y^k$ in $\mathbb{F}_q$. For each $x \neq 0$ there are k solutions for y so

$$S_2 = q((q-1)k+1).$$

Similarly we obtain

$$S_2^* = q(q-1)k.$$

The estimates for S_c and S_c^* follow from the estimates for S_2 and S_2^* with p replaced by q as does the rest of the argument, and we obtain a non-singular solution to the equations provided that

$$\begin{aligned} q &> r^2k^{2+\frac{2}{c-2}}, \qquad r \neq 1 \\ q &> k^{2+\frac{2}{c-1}}, \qquad r = 1. \end{aligned}$$

5.7 Applications to Artin's conjecture

For the equations (5.1) Artin's conjecture is the case $c = k$. Thus for $r > 1$ our theorem gives a non-trivial p-adic solution for $p > r^2k^{2+\frac{2}{k-2}}$, $r \neq 1$. Thus for cubic equations we have $p > r^2 3^4 = 91r^2$, for quartic equations we have $p > r^2 4^3 = 64r^2$ and for quintic equations we have $p > r^2 5^{2+\frac{2}{3}} \approx 73.2r^2$.

Part III

Graph Theory

Chapter 6

Basic Preliminaries

In this chapter we review some basic definitions and concepts that will be useful to us in this part of the thesis.

6.1 Definitions

If Y is a set, then the power set of Y is the set of all subsets of Y. It is denoted by $P(Y)$.

A graph G consists of a set V (or $V(G)$) of vertices, a set E (or $E(G)$) of edges, and a relation of incidence that associates with each edge two vertices, called its ends. A graph is simple when it has no loops and no two distinct edges have exactly the same pair of ends. In this thesis all graphs we consider shall be simple.

A set system (on Y) is a pair (Y, F), where Y is a set and $F \subset P(Y)$, and an r-graph or r-uniform hypergraph is a pair (Y, ξ) where $\xi \subset Y^{(r)}$. An element of ξ is a hyperedge or simply an edge of the hypergraph. Thus we see that a graph, as defined in the paragraph above, is a 2-graph.

If Γ is a graph then the degree or valency of a vertex X is the number of edges on X or, equivalently, the number of vertices 'adjacent to ' X.

If each vertex has the same degree d, then the graph is said to be regular, of degree d.

Let Γ be a regular graph of degree k, with v vertices. If there are integers λ, μ, such that:

1. if P, Q are adjacent vertices, then there are exactly λ vertices X adjacent to both P and Q.

2. if P, Q are non-adjacent (distinct) vertices, then there are exactly μ vertices X adjacent to both P and Q.

Then Γ is a strongly regular graph with parameters (v, k, λ, μ).

We use K_n to denote the complete graph on n vertices.

An $n \times n$ matrix $\mathbf{H}$ is a Hadamard matrix of order n if each entry is 1 or -1, and $\mathbf{HH^T} = n\mathbf{I}$.

6.2 Ramsey theory

In 1930 F.P.Ramsey published a paper on logic which contained the following theorem [53]:

Theorem 34 *Let $r \geq 1$ and $q_i \geq r$, $i = 1, 2, \ldots, s$ be given. There exists a minimal positive integer $N(q_1, q_2, \ldots, q_s; r)$ with the following property. Let S be a set with n elements. Suppose that all $\binom{n}{r}$ r-subsets of S are divided into s mutually exclusive families $T_1, \ldots, T_s$ ('colours'). Then if $n \geq N(q_1, q_2, \ldots, q_s; r)$ there is an i, $1 \leq i \leq s$, and some q_i-subset of S for which every r-subset is in T_i.*

This seems a rather technical statement and as all our applications will be to hypergraphs and graphs we shall re-interpret the result for these structures. Basically Ramsey's Theorem states that if you colour the edge sets of the complete r-uniform hypergraph on n vertices with s colours then if $n \geq N(q_1, q_2, \ldots, q_s; r)$ you will always find, for some i, a monochromatic sub-hypergraph of colour i and size q_i. For example $N(3, 3; 2) = 6$ means that if you colour the edges of K_6 with either red or blue you will find at least one monochromatic triangle.

Chapter 7

Diagonal Equations and Graph Theory

In this chapter I should like to investigate the connections between the theory of graph colourings and the preceding theory of diagonal congruences.

7.1 Introduction

Let us begin with a problem concerning the solution of diagonal congruences with a fixed number of variables non-zero. Consider two diagonal equations over the finite field $\mathbb{F}_q$, q a prime power

$$\begin{aligned} f &= a_1x_1^k + \cdots + a_nx_n^k = 0 \\ g &= b_1x_1^k + \cdots + b_nx_n^k = 0 \end{aligned} \tag{7.1}$$

whose columns happen to be in general position, i.e. $a_ib_j - b_ia_j \neq 0$ for all i, j. The question is : does (7.1) have a solution with exactly 3 variables non-zero? It is perhaps quite surprising that the solution to this question lies in the world of combinatorics and Ramsey Theory. In fact for q greater than some bound it can be shown that there is a direct equivalence between the problem of finding monochromatic triangles in graphs and obtaining a solution in exactly 3 variables.

7.2 Algebraic preliminaries

Let q be a prime power, k a positive integer greater than 1 and $q \equiv 1 \pmod{k}$. Then the group $\mathbb{F}_q^*$ contains a subgroup consisting of kth powers, $R = \left\{x^k : x \in \mathbb{F}_q^*\right\}$, with $|R| = \frac{q-1}{k}$. This subgroup can then be used to decompose $\mathbb{F}_q^*$ into a disjoint union of k cosets:

$$\mathbb{F}_q^* = \bigcup_{i=1}^{k} g^i R = \bigcup_{i=1}^{k} A_i$$

where g is an element of $\mathbb{F}_q^*$ such that $g^j \notin R$ for $j = 1, \ldots, k-1$ and $A_i = g^i R$.

7.3 The associated graph

As in the introduction let us consider the pair of equations

$$\begin{aligned} f &= a_1 x_1^k + \cdots + a_n x_n^k = 0 \\ g &= b_1 x_1^k + \cdots + b_n x_n^k = 0 \end{aligned} \tag{7.2}$$

with independent columns over $\mathbb{F}_q$, $q = p^s$, p prime, $q \equiv 1 \pmod{k}$ if k is odd, and $q \equiv 1 \pmod{2k}$ if k is even. We also note that the condition of independent columns requires that $q \geq n+1$.

We shall show how the coset decomposition of $\mathbb{F}_q^*$ gives us an edge colouring of the complete graph on n vertices in k colours.

Take the complete graph on n vertices and label each vertex from $1, \ldots, n$. Then to the vertex i we associate the column $\begin{pmatrix} a_i \\ b_i \end{pmatrix}$. We then 'colour' the edges of the graph with the numbers from $1, \ldots, k$ by the rule:

edge $i-j$ is assigned colour t if and only if $a_i b_j - b_i a_j \in A_t$.

This makes sense since for the values of q we have defined -1 is a kth power, and hence edge $i-j$ is assigned the same colour as edge $j-i$.

Example 35 *Consider the equations*

$$\begin{aligned} f &= x_1^k + \quad + x_3^k = 0 \\ g &= \qquad x_2^k + x_3^k = 0 \end{aligned}$$

Then the three cross products $a_ib_j - b_ia_j$ *are* $1, 1, -1$, *so the equation graph is* K_3 *with each edge coloured 1.*

Now let us return to the problem mentioned in the introduction. What does it mean for (7.2) to have a solution with exactly 3 variables non-zero?

Let us assume that we have a solution with only the variables r, s, t non-zero. This means we have a solution with all variables non-zero to

$$\begin{aligned} a_rx_r^k + a_sx_s^k + a_tx_t^k &= 0 \\ b_rx_r^k + b_sx_s^k + b_tx_t^k &= 0. \end{aligned} \tag{7.3}$$

Now simple linear algebra tells us that this solution must be given by

$$(x_r^k : x_s^k : x_t^k) = (a_sb_t - b_sa_t : a_tb_r - b_ta_r : a_rb_s - b_ra_s).$$

This is possible if and only if $a_sb_t - b_sa_t$, $a_tb_r - b_ta_r$, $a_rb_s - b_ra_s$ are all in the same coset A_u of the group R of kth powers. On the graph this corresponds to the edges $r - s$, $s - t$ and $t - r$ all having colour u. Thus we have a monochromatic triangle and the following theorem holds

Theorem 36 *The equations (7.2) have a solution with exactly three variables non-zero if and only if the associated graph of the equation has a monochromatic triangle.*

7.4 Monochromatic triangles

We know that Ramsey's Theorem guarantees the existence of $N(w_1, w_2, \ldots, w_k; 2)$, the least integer n with the property that for every k-colouring of the edges of K_n, there exists an i,

$1 \leq i \leq k$, and a complete subgraph K_{w_i} of K_n having all edges coloured by the ith colour.

We are interested in the special case $w_1 = w_2 = \cdots = w_k = 3$. Denote $N(\overbrace{w, w, \ldots, w}^{k}; 2)$ by $r(w; k)$. Then if $s \geq r(3; k)$, every edge colouring in k colours of the complete graph on s vertices possesses a monochromatic triangle.

Thus if $n \geq r(3; k)$, the pair of equations (7.2) has a solution with exactly 3 variables non-zero. Bounds for r have also been derived:

Theorem 37

$$\frac{3^t + 3}{2} \leq r(3; t) \leq \lfloor t!e \rfloor \ , \ t \geq 4$$

Proof. See [35, pp.127-128].

Now we know that Chevalley's Theorem (Chapter 1, Theorem 2) gives a non-trivial solution to (7.2) for all $n > 2k$, making the bounds for r seem surprisingly high. This difference could be said to be a result of two factors:

1. $N^{\min}$ comes from looking at all possible edge colourings of the complete graph, not just the ones arising from equations. Therefore our equation may be soluble with exactly three variables non-zero for a much smaller value of n.
2. Chevalley's theorem asks for any non-trivial solution, not just one with exactly three variables non-zero. Hence it may be the case that the latter solution is much harder to obtain than the former.

The first point really comes down to the question: 'Does every graph colouring arise from some pair of additive equations?'. If we assume conjecture 14 on the generalised Hasse-Weil sum estimate the answer is yes for $q > 4n^2k^{n+1}$, since q has to be large enough to enable the equations to encode enough information about the colourings. We shall demonstrate this in chapter 9 . Let me illustrate my statement with a rough heuristic estimate:

First let us restrict our attention to the particular equation

$$\begin{aligned} x_1^k + \cdots + x_n^k &= 0 \\ a_1 x_1^k + \cdots + a_n x_n^k &= 0 \end{aligned} \tag{7.4}$$

with all the a_i's distinct so that we have independent columns. Then the colouring procedure is simple:

$$i - j \text{ has colour } t \iff a_i - a_j \in A_t$$

Now we make two estimates

1. Total number of colourings $\approx k^{\binom{n}{2}}$.
2. Total number of equations $\approx q^n$.

Thus for every colouring to have an equation we require

$$q^n > k^{\binom{n}{2}} \text{or } q > k^{\frac{1}{2}(n-1)}.$$

Returning to the second point, we now see that for large q at least, this is what must explain the comparatively high bounds for r.

7.5 A bound for q

We shall prove the following theorem in Chapter 9, assuming conjecture 14:

Theorem 38 *Let c_{ij} be an arbitrary colouring of the complete graph on n vertices. If conjecture 14 is true then there is an equation of degree k which corresponds to this graph colouring if*

$$q > 4n^2k^{n+1}, \qquad k \geq 3 \tag{7.5}$$

$$q > n^2 2^{n+2}, \qquad k = 2 \tag{7.6}$$

Thus we see that we have a direct equivalence between the graph colouring and the equations expressed in the following theorem:

Theorem 39 *Let $N_{eqn}^{\min}(k)$ be the minimum value of n such that the equations (7.2) have a solution with exactly 3 variables non-zero for all q and all values of the a_i's; then*

$$N_{eqn}^{\min}(k) = N^{\min}(k).$$

Proof. Theorem 36 shows that $N^{\min}_{eqn}(k) \leq N^{\min}(k)$. Now if $n < N^{\min}(k)$ there exists a k-colouring on n vertices with no monochromatic triangle. By theorem 38, if $q > 4n^2k^n$, there is an equation with n variables which corresponds to this graph and hence has no solution with exactly 3 variables non-zero. This shows that $N^{\min}_{eqn}(k) \geq N^{\min}(k)$ and the result follows.

An alternative form of this asking for non-trivial solutions is

Theorem 40 *Let $N^{\min}_{eqn}(k)$ be the minimum value of n such that the equations*

$$\begin{aligned} a_1x_1^k + \cdots + a_nx_n^k &= 0 \\ b_1x_1^k + \cdots + b_nx_n^k &= 0 \\ x_1^{q-1} + \cdots + x_n^{q-1} - 3x_{n+1}^{q-1} &= 0 \end{aligned} \tag{7.7}$$

have a non-trivial solution for all q and all values of the a_i's, $a_ib_j - a_jb_i \neq 0$, then

$$N^{\min}_{eqn}(k) = N^{\min}(k).$$

Proof. We simply have to show that any non-trivial solution of the equations (7.7) has exactly 3 variables non-zero from $x_1, \ldots, x_n$. Since $\mathbb{F}_q^*$ is a cyclic group of order $q-1$, the values of x^{q-1}, $x \in \mathbb{F}_q$ are 0 or 1. Now, since $a_ib_j - a_jb_i \neq 0$ for all $1 \leq i, j \leq n$ we must have $n+1 \leq q$. Thus a non-trivial solution to $x_1^{q-1} + \cdots + x_n^{q-1} - 3x_{n+1}^{q-1} = 0$ cannot have $x_{n+1} = 0$. Hence we are solving $x_1^{q-1} + \cdots + x_n^{q-1} = 3$ which implies exactly 3 out of $x_1, \ldots, x_n$ are non-zero.

7.6 Generalisation to more than two equations

Consider a set of r diagonal equations over $\mathbb{F}_q$:

$$f_i = a_{i1}x_1^k + \cdots + a_{in}x_n^k = 0, \qquad 1 \leq i \leq r, \tag{7.8}$$

with $q \equiv 1 \pmod{k}$ if k is odd, and $q \equiv 1 \pmod{2k}$ if k is even. Also let each $r \times r$ submatrix have non-zero determinant.

Then in this case we wish to look at solutions with exactly $r+1$ variables non-zero. Now let us look at the graph colouring.

7.6.1 The associated graph colouring

We wish to define a colouring of the faces of the complete graph K_n on n vertices. By face I mean a set of r vertices of K_n. Using the definitions in Chapter 6, we see that this can be considered as a colouring of the hyperedges of the r-graph on n vertices.

As before take K_n and label the vertices from $1,\ldots,n$. Then to the vertex j we associate the column $(a_{1j},\ldots,a_{rj})^{\mathrm{T}}$. Each face is defined by the r vertices that lie in it. We then colour the faces according to the rule:

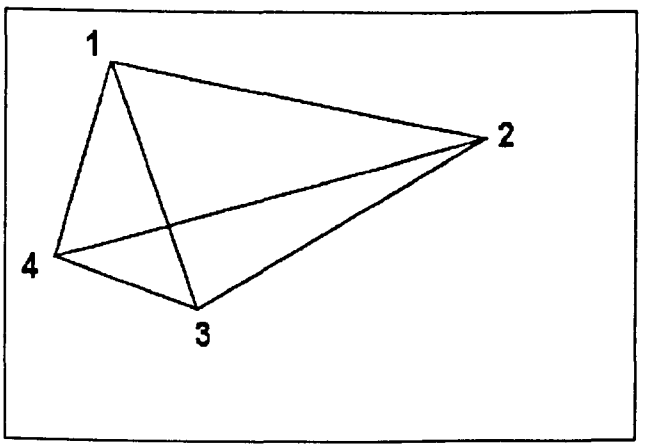
> the face with vertex set S is assigned colour t if and only if
>
> the determinant of the $r \times r$ submatrix defined by S lies in A_t.

This makes sense again since any permutation of the vertices multiplies the determinant by ± 1 and for our values of q, -1 is a k-th power.

Example 41 *Consider the equation*

$$\begin{aligned} f = x_1^k + \quad & +x_4^k = 0 \\ g = \quad x_2^k + \quad & +x_4^k = 0 \\ h = \quad & x_3^k + x_4^k = 0. \end{aligned}$$

Then the four determinants are $1,1,1,1$, *so the equation graph is*



with each face coloured k.

Now let us return to the problem of solving an equation with exactly $r+1$ variables non-zero. First consider the $r \times (r+1)$ matrix formed by the columns of these variables. Then the equivalent condition is that the $r+1$ determinants of the $r+1$ $(r \times r)$ submatrices all have values in the same coset, A_u say. On the graph this corresponds to the $r+1$ faces all having colour u. Thus we see that the following theorem holds

Theorem 42 *The equations (7.8) have a solution with exactly $r+1$ variables non-zero if and only if the associated r-graph of the equation has a monochromatic set of $r+1$ vertices.*

Chapter 8

The Paley Graph

Let us now define the Paley graph and see how this can be generalised to colourings and to hypergraphs. Then, as a consequence of the above work we shall prove some theorems about subgraphs and subcolourings.

8.1 Main properties of P_q

The Paley graph, P_q, where q is a prime power, p^s, is defined only for $q \equiv 1 \pmod 4$. This means that -1 is a quadratic residue in $\mathbb{F}_q$. It possesses q vertices corresponding to the elements of $\mathbb{F}_q$. The traditional definition is phrased by saying that two vertices a, b are joined if and only if $a - b$ is a quadratic residue. This makes sense because -1 is a square in $\mathbb{F}_q$.

The original construction of Paley was not of P_q but of the related Paley tournament $\vec{P}_q$, and his main interest was that $\vec{P}_q$ could be used to construct Hadamard matrices of order $q+1$, where $q \equiv -1 \pmod 4$. $\vec{P}_q$ is simply defined by saying that an arc from a to b exists if and only if $a - b$ is a quadratic residue. Obviously this only makes sense if $q \equiv -1 \pmod 4$, in which case -1 is a quadratic non-residue.

The Paley graph P_q can also be used to define a $(q+1) \times (q+1)$ orthogonal matrix which is close to a Hadamard matrix. What is also remarkable about P_q is that it possesses many beautiful properties which makes it closely resemble a random subgraph of the complete graph in which each edge occurs with probability 1/2. For example one sees that the degree of every vertex is about $q/2$. We shall now introduce some of the properties of the Paley graph and

tournament and some related combinatorial constructions.

Theorem 43 *The graph P_q is a doubly transitive, self-complementary, strongly regular graph with parameters $\{(q-1)/2, (q-5)/4, (q-1)/4\}$. That is to say, P_q is $(q-1)/2$ - regular, any two vertices have $(q-5)/4$ common neighbours and any two non-adjacent vertices have $(q-1)/4$ common neighbours. For any two vertices a and b, there are precisely $(q-1)/4$ vertices $c \neq b$ joined to a and not joined to b.*

We repeat for completeness the proof in Bollobas [11], p 316.

Proof. Multiplication of the edge set by a quadratic non-residue maps P_q into its complement, so P_q is self-complementary.

Given edges uv and $u'v'$ there is a linear function $\phi : \mathbb{F}_q^2 \to \mathbb{F}_q^2$, $\phi(x) = ax + b$, mapping u to u' and v to v'. Then $\chi(a) = \chi(a)\chi(u-v) = \chi(a(u-v)) = \chi\left(u'-v'\right) = 1$, so ϕ gives an automorphism of P_q, mapping u to u' and v to v'. Hence P_q is doubly transitive.

Let $x \in \mathbf{V}(P_q)$, $U = \Gamma(x)$, $W = V(P_q)\backslash(U \cup \{x\})$ and $q = 4k+1$. We know that each vertex $y \in U$ is joined to the same number of vertices in W, say l, and also that each vertex $z \in W$ is not joined to precisely l vertices in U. Then

$$|U|\,|W| = (2k)^2 = 2kl + 2kl,$$

so $l = k$. Therefore any two adjacent vertices have $k-1$ common neighbours and any two non-adjacent vertices have k common neighbours. Since P_q is self-complementary, for any two non-adjacent vertices there are $k-1$ other vertices joined to neither of them, and for any two adjacent vertices there are k vertices joined to neither of them.

Finally, for any two vertices a, b there are $2k$ vertices, distinct from a and b, joined to precisely one of them. Since P_q has an automorphism interchanging a and b, of these $2k$ vertices k are joined to a and not to b, and k are joined to b and not to a. ■

A tournament T is *arc-homogeneous* if, for each pair of arcs uv and xy, there is an automorphism of T taking u to x and v to y. Goldberg [34] proved the following result which was rediscovered independently by Berggren [7].

Theorem 44 *The automorphism group of the quadratic residue tournament $\vec{P}_q$ consists of all permutations π with*

$$\pi(x) = a^2\alpha(x) + c$$

where α is an automorphism of the field $\mathbb{F}_q$ and a, c are elements of $\mathbb{F}_q$ with $a \neq 0$.

Fried [33] has observed that, for any arcs ij and hk in $\vec{P}_q$, the permutation

$$\pi(x) = \frac{(k-h)}{(j-i)}x + \left(h - \frac{(k-h)}{(j-i)}i\right)$$

sends i to h and j to k. Further, it is easy to see that $(k-h)/(j-i)$ is a quadratic residue, and therefore π is an automorphism of $\vec{P}_q$. Thus every quadratic residue tournament is arc-homogeneous; Berggren [7] has established that they are the only ones.

Theorem 45 *A tournament with n (≥ 3) vertices is arc-homogeneous if and only if it is a quadratic residue tournament.*

As we mentioned above Paley's original construction was of the Paley tournament, which he used to construct Hadamard matrices. Let $\mathbf{A} = (a_{ij})$ be the adjacency matrix of the Paley tournament $\vec{P}_q$. Then

$$a_{ij} = \chi(i-j)$$

where χ is the quadratic residue character , and i, j are elements of $\mathbb{F}_q$. Let $\mathbf{B} = \mathbf{A} - \mathbf{I}$, where $\mathbf{I}$ is the identity matrix of order q. A Hadamard matrix $\mathbf{H}$ of order $q+1$ can be formed by adding a border of 1's as the first row and column to the matrix $\mathbf{B}$. This follows easily from the analogue of theorem 43:

Theorem 46 *The tournament $\vec{P}_q$ is arc-homogeneous. Also it is equal to the graph formed by reversing the directions of all its arcs, and is strongly regular in the following sense: If a and b are vertices of $\vec{P}_q$ then (ab) means there is an arc from a to b. For any two vertices satisfying (ab) there are k vertices c with (bc) and (ca) and $k-1$ vertices c with (cb) and (ca). Since $\vec{P}_q$ is self-complementary, for any two vertices satisfying (ab) there are k vertices c with (cb) and (ac) and $k-1$ vertices c with (bc) and (ac).*

Proof. Multiplication by a quadratic non-residue maps $\vec{P}_q$ into the graph formed by reversing the directions of all its arcs.

Given arcs (uv) and $(u'v')$ there is a linear function $\phi : \mathbb{F}_q^2 \to \mathbb{F}_q^2$, $\phi(x) = ax + b$, mapping u to u' and v to v'. Then $\chi(a) = \chi(a)\chi(u - v) = \chi(a(u - v)) = \chi\left(u' - v'\right) = 1$, so ϕ gives an automorphism of $\vec{P}_q$, mapping u to u' and v to v'. Hence $\vec{P}_q$ is arc homogeneous.

Let $x \in \mathbf{V}(\vec{P}_q)$, $U = \left\{y \in \mathbf{V}(\vec{P}_q) : (xy)\right\}$, $W = V(\vec{P}_q)\backslash(U \cup \{x\})$ and $q = 4k - 1$. We know that each vertex $y \in U$ satisfies (yw) for the same number of vertices $w \in W$, say l, and also that each vertex $w \in W$ satisfies (wz) for precisely $l - 1$ vertices $z \in U$. Then

$$|U|\,|W| = (2k-1)^2 = (2k-1)l + (2k-1)(l-1),$$

so $l = k$. Therefore for any two vertices satisfying (ab) there are k vertices c with (bc) and (ca) and $k - 1$ vertices c with (cb) and (ca). Since $\vec{P}_q$ is self-complementary, for any two vertices satisfying (ab) there are $k - 1$ vertices c with (bc) and (ac).

Finally let $x \in \mathbf{V}(\vec{P}_q)$, $y \in U = \left\{y \in \mathbf{V}(\vec{P}_q) : (xy)\right\}$. Then there are $k - 1$ $y' \in U$ with (yy') and $k - 1$ with $(y'y)$. Thus for any two vertices satisfying (ab) there are $k - 1$ vertices c with (ac) and (cb).

This gives an explicit construction of Hadamard matrices of order $q + 1$ whenever q is a power of a prime and $q \equiv 3 \pmod 4$.

Theorem 47 *Let* $\mathbf{A}$ *be the adjacency matrix of the Paley tournament* $\vec{P}_q$. *Let* $\mathbf{A} - \mathbf{I}$, *where* $\mathbf{I}$ *is the identity matrix of order* q. *A Hadamard matrix* $\mathbf{H}$ *of order* $q+1$ *can be formed by adding a border of 1's as the first row and column to the matrix* $\mathbf{B}$.

Proof. $\chi(-1) = -1$, therefore $\mathbf{A}$ is skew symmetric and $\mathbf{A} + \mathbf{A}^{\mathbf{T}} = \mathbf{0}$. Let $\mathbf{B} = \mathbf{A} - \mathbf{I}$, where $\mathbf{I}$ is the identity matrix of order q. Then

$$\begin{aligned}\mathbf{B}\mathbf{B}^{\mathbf{T}} = (\mathbf{A}-\mathbf{I})(\mathbf{A}-\mathbf{I})^{\mathbf{T}} = (\mathbf{A}-\mathbf{I})\left(\mathbf{A}^{\mathbf{T}}-\mathbf{I}\right) &= \mathbf{A}\mathbf{A}^{\mathbf{T}} - \mathbf{A}^{\mathbf{T}} - \mathbf{A} + \mathbf{I} \\ &= -\mathbf{A}^2 + \mathbf{I}\end{aligned}$$

Now the ijth element of $\mathbf{A}^2$ is given by

$$\left(\mathbf{A}^2\right)_{ij} = \#\left\{c \in \vec{P}_q : (ic) \;\&\; (cj) \text{ or } (jc) \;\&\; (ci)\right\} - \#\left\{c \in \vec{P}_q : (ic) \;\&\; (jc) \text{ or } (cj) \;\&\; (ci)\right\}$$

By Theorem 46 this reduces to

$$\begin{aligned}\left(\mathbf{A}^2\right)_{ij} &= k-1+k-(k-1)-(k-1) \\ &= 1, \qquad i \neq j\end{aligned}$$

and

$$\left(\mathbf{A}^2\right)_{ii} = -(q-1).$$

Hence,

$$\begin{aligned}\left(\mathbf{B}\mathbf{B}^{\mathbf{T}}\right)_{ij} &= -1, \qquad i \neq j \\ \left(\mathbf{B}\mathbf{B}^{\mathbf{T}}\right)_{ii} &= q\end{aligned}$$

Now the Hadamard Matrix $\mathbf{H}$ is obtained from $\mathbf{B}$ by adding a column of 1's and a row of 1's. Thus it is easy to see that

$$\begin{aligned}\left(\mathbf{H}\mathbf{H}^{\mathbf{T}}\right)_{ij} &= \left(\mathbf{B}\mathbf{B}^{\mathbf{T}}\right)_{ij} + 1 = 0, \qquad i \neq j, 1 \leq i, j \leq q \\ \left(\mathbf{H}\mathbf{H}^{\mathbf{T}}\right)_{ii} &= \left(\mathbf{B}\mathbf{B}^{\mathbf{T}}\right)_{ii} + 1 = q+1, \qquad 1 \leq i \leq q\end{aligned}$$

Since each vertex of $\vec{P}_q$ has the same number of arcs entering as leaving, the remaining elements of $\mathbf{H}$ can be calculated to give $\mathbf{H}\mathbf{H}^{\mathbf{T}} = (q+1)\mathbf{I}$. Thus $\mathbf{H}$ is a Hadamard matrix. ■

Alternative Proof: A simpler, but less graph-theoretic proof proceeds as follows:

Proof. We calculate $\mathbf{A}^2$ using the quadratic characters, χ. Then

$$\begin{aligned}\left(\mathbf{A}^2\right)_{ik} &= \sum_{j=1}^{q} \chi(i-j)\chi(j-k) = \sum_{j=1}^{q} \chi(j)\chi(i-j-k) \\ &= \sum_{j=1}^{q} \chi(j)\chi(i-k-j) = \sum_{j=1}^{q} \chi(j)\chi(1-j)\end{aligned}$$

$$= \sum_{j=1}^{q-1} \chi(\frac{1}{j})\chi(1-\frac{1}{j}) = \sum_{j=1}^{q-1} \chi(j-1)$$
$$= \sum_{j=0}^{q-2} \chi(j) = \sum_{j=0}^{q-1} \chi(j) - \chi(-1) = 1, \qquad i \neq k$$

The rest of the proof then follows as before. ■

One reason why random graphs are useful is that they possess subgraphs of various kinds. This is investigated in the next chapter.

8.2 The generalised Paley c-graph

Before we begin I should like to define what I mean by a colour-graph or c-graph. A c-graph is an ordinary graph with an associated colouring of the edges. Also a sub c-graph is simply a subgraph of a c-graph with the induced colouring.

The generalised Paley c-graph P_q^k has q vertices corresponding to the q elements of $\mathbb{F}_q$. As for the Paley Graph we need conditions on q to ensure -1 is a kth power, $q \equiv 1 \pmod{k}$ if k is odd and $q \equiv 1 \pmod{2k}$ if k is even. To the graph we associate a k-colouring given by

$$\text{edge } i-j \text{ is assigned colour } t \text{ if and only if } i-j \in A_t.$$

Now a subc-graph is simply a subgraph of a c-graph with the induced colouring. Let us now consider what analogies we can draw, and hopefully prove, between the graph P_q and the c-graph P_q^k. First of all P_q^k again seems to resemble a random graph, only this time it is a random c-graph where each edge colour occurs with probability $1/k$. As we found above, is there a number s such that every c-graph with s vertices is contained in P_q^k ? The expected value for s is $(1+o(1))\frac{2\log q}{\log k}$. In the chapter on r-fullness we shall investigate this further.

Looking back at the pairs of equations and their associated graph in chapter 6 we see that the Paley graph is really the graph of an equation with $a_i = 1$ and $b_i = i$, $1 \leq i \leq p$. Thus the question naturally arises whether it is possible to generalise P_q using this observation. The answer is yes as we shall see in section 8.3.1.

8.3 Points at infinity, P_q, $\vec{P}_q$ and Hadamard matrices

Let us now see what happens if we add an extra point to the graphs P_q and $\vec{P}_q$. At first glance there seem to be no remaining elements of $\mathbb{F}_q$ to use. Instead we add what will be called a 'point at infinity', ∞. This point has the property that every vertex is connected to it by an edge in P_q, and there is an arc from it to every other point in $\vec{P}_q$. Later, when we have defined the extended Paley graph and tournament, the terminology will be seen to be appropriate. Now note here that the introduction of ∞ corresponds to adding an extra row of 1's and a column of 1's to the adjacency matrix of $\vec{P}_q$. This is crucial step in constructing a Hadamard matrix.

8.3.1 A new graph

We shall now define a new graph M_q of degree q where q is a prime power and $q \equiv 1 \pmod 4$. Let $a_i, b_i \in \mathbb{F}_q$,$1 \leq i \leq q+1$ be such that $a_i b_j - a_j b_i \neq 0$ for all $i \neq j$. Then M_q has vertex set $\begin{pmatrix} a_i \\ b_i \end{pmatrix}$ and vertex i is joined to vertex j if and only if $a_i b_j - a_j b_i$ is a quadratic residue. We note the obvious fact that M_q is not unique and depends on the vertex set selected.

If $q \equiv 3 \pmod 4$ then we can define an extension of the Paley tournament, $\vec{M}_q$: the vertex set of $\vec{M}_q$ is the same as M_q and there is an arc from vertex i to vertex j if and only if $a_i b_j - a_j b_i$ is a quadratic residue.

Let $\mathbf{A} = (a_{ij})$ be the adjacency matrix of the tournament $\vec{M}_q$. Then

$$a_{ij} = \chi(a_i b_j - a_j b_i)$$

where χ is the quadratic residue character, and i, j are elements of $\mathbb{F}_q$. Let $\mathbf{B} = \mathbf{A} - \mathbf{I}$, where $\mathbf{I}$ is the identity matrix of order q. This is a Hadamard matrix of order $q+1$. Unfortunately $\mathbf{B}$ does not really give us a new Hadamard matrix, since it can be obtained from our Paley matrix by multiplying certain rows and columns by -1. However, this method does make Paley's construction less artificial and gives clues to higher dimensional generalisations.

8.3.2 Some properties of M_q and $\vec{M}_q$

We give a proof that $\vec{M}_q$ can be used to construct Hadamard matrices:

Theorem 48 *Let $a_i, b_i \in \mathbb{F}_q$,$1 \leq i \leq q+1$, $q \equiv 3 \pmod 4$, be such that $a_ib_j - a_jb_i \neq 0$ for all $i \neq j$. Form the matrix $\mathbf{M} = (m_{ij}) = \chi(a_ib_j - a_jb_i)$. Then the matrix $\mathbf{H} = \mathbf{M} - \mathbf{I}$, where $\mathbf{I}$ is the identity matrix of order $q+1$ is a Hadamard matrix.*

Note that $\mathbf{M}$ is the adjacency matrix for $\vec{P}_q$ with an extra point, forming a new tournament that contains vertex points corresponding to the $q+1$ points of the projective line $\mathbb{P}(\mathbb{F}_q)$.

Proof. $\chi(-1) = -1$ and $m_{ii} = 0$ therefore $\mathbf{M}$ is skew symmetric and $\mathbf{M} + \mathbf{M}^{\mathbf{T}} = \mathbf{0}$. Hence

$$\begin{aligned}\mathbf{HH^T} &= (\mathbf{M}-\mathbf{I})(\mathbf{M}-\mathbf{I})^{\mathbf{T}} = (\mathbf{M}-\mathbf{I})\left(\mathbf{M^T}-\mathbf{I}\right) = \mathbf{MM^T} - \mathbf{M^T} - \mathbf{M} + \mathbf{I} \\ &= -\mathbf{M^2} + \mathbf{I}.\end{aligned}$$

$$\left(\mathbf{M}^2\right)_{ik} = \sum_{j=1}^{q+1} \chi(a_ib_j - a_jb_i)\chi(a_jb_k - a_kb_j).$$

Now if we multiply each vector $\begin{pmatrix} a_i \\ b_i \end{pmatrix}$ by a non-zero scalar λ_i and evaluate the above sum we obtain

$$\begin{aligned}&\sum_{j=1}^{q+1} \chi(\lambda_ia_i\lambda_jb_j - \lambda_ja_j\lambda_ib_i)\chi(\lambda_ja_j\lambda_kb_k - \lambda_ka_k\lambda_jb_j) \\ &= \sum_{j=1}^{q+1} \chi(\lambda_i\lambda_j^2\lambda_k)\chi(a_ib_j - a_jb_i)\chi(a_jb_k - a_kb_j) \\ &= \chi(\lambda_i\lambda_k)\sum_{j=1}^{q+1} \chi(a_ib_j - a_jb_i)\chi(a_jb_k - a_kb_j) \\ &= \chi(\lambda_i\lambda_k)\left(\mathbf{M}^2\right)_{ik}. \qquad (8.1)\end{aligned}$$

Since $\left\{\begin{pmatrix} a_i \\ b_i \end{pmatrix} : 1 \leq i \leq q+1\right\}$ is a complete list of representatives of $\mathbb{P}(\mathbb{F}_q)$, by multiplying the vectors by suitable scalars λ_i we obtain the set $\left\{\begin{pmatrix} 0 \\ 1 \end{pmatrix}, \begin{pmatrix} 1 \\ 0 \end{pmatrix}, \begin{pmatrix} 1 \\ 2 \end{pmatrix}, \ldots, \begin{pmatrix} 1 \\ q \end{pmatrix}\right\}$. Since we seek to prove $\mathbf{M}_{ik}^2 = 0$ $i \neq j$ then we may take

$$\left\{\begin{pmatrix} a_i \\ b_i \end{pmatrix} : 1 \leq i \leq q+1\right\} = \left\{\begin{pmatrix} 0 \\ 1 \end{pmatrix}, \begin{pmatrix} 1 \\ 0 \end{pmatrix}, \begin{pmatrix} 1 \\ 2 \end{pmatrix}, \ldots, \begin{pmatrix} 1 \\ q \end{pmatrix}\right\}.$$

Also if $\begin{pmatrix} a_i' \\ b_i' \end{pmatrix} = \mathbf{L} \begin{pmatrix} a_i \\ b_i \end{pmatrix}$ we have

$$a_i'b_j' - a_j'b_i' = \det(\mathbf{L})(a_ib_j - a_jb_i),$$

so

$$\begin{aligned} & \sum_{j=1}^{q+1} \chi(a_i'b_j' - a_j'b_i')\chi(a_j'b_k' - a_k'b_j') \\ = & \sum_{j=1}^{q+1} \chi(\det(\mathbf{L})(a_ib_j - a_jb_i))\chi(\det(\mathbf{L})(a_jb_k - a_kb_j)) \\ = & \sum_{j=1}^{q+1} \chi(\det{}^2(\mathbf{L})(a_ib_j - a_jb_i))\chi(a_jb_k - a_kb_j) \\ = & \sum_{j=1}^{q+1} \chi(a_ib_j - a_jb_i)\chi(a_jb_k - a_kb_j). \end{aligned}$$

Now there exists a non-singular matrix $\mathbf{L}$ which sends $\begin{pmatrix} a_i \\ b_i \end{pmatrix}$ to $\begin{pmatrix} 0 \\ 1 \end{pmatrix}$ and $\begin{pmatrix} a_j \\ b_j \end{pmatrix}$ to $\begin{pmatrix} 1 \\ 0 \end{pmatrix}$.
Thus in evaluating $\mathbf{M}_{ik}^2$ we can take $a_i = b_j = 0$ and $b_i = a_j = 1$. Thus

$$\mathbf{M}_{ik}^2 = \sum_{j=1}^{q+1} \chi(-1)\chi(b_k) = 0.$$

Hence

$$\begin{aligned} \mathbf{M}_{ik}^2 &= 0, \qquad i \neq k \\ \mathbf{M}_{ii}^2 &= -q, \end{aligned}$$

giving $\mathbf{H}\mathbf{H}^{\mathbf{T}} = (q+1)\mathbf{I}$ and $\mathbf{H}$ is a Hadamard matrix.

Our construction includes the one from $\vec{P}_q$ as the special case $a_i = 1$, $b_i = i$, $1 \leq i \leq q$.

8.4 A hyper Paley graph

The above ideas suggest that we may be able to generalise the Paley graph to hypergraphs. We have seen that the usual definition of P_q can be replaced by taking a vertex set

$$\left\{\begin{pmatrix}1\\0\end{pmatrix},\begin{pmatrix}1\\2\end{pmatrix},\ldots,\begin{pmatrix}1\\q\end{pmatrix}\right\}$$

and saying that two vertices are connected if the determinant formed by their vectors is a quadratic residue. In this case the linear transformation $\phi : \mathbb{F}_q \to \mathbb{F}_q$, $\phi(x) = ax + b$ becomes

$$\varphi : \mathbb{F}_q^2 \to \mathbb{F}_q^2, \varphi(\mathbf{x}) = \begin{pmatrix}1 & 0\\ b & a\end{pmatrix}\mathbf{x}. \tag{8.2}$$

The difficulty in finding an appropriate generalisation to hypergraphs is that it is difficult to find large sets of vectors $\in \mathbb{F}_q^r$ which are in general position (any set of r vectors are independent) and which also possess good automorphism properties. We shall settle for a set of vectors which have some faces with vanishing determinant, but which have automorphisms similar to the above example:

The r-graph generalisation of the Paley graph I denote by P_q^r. This is a graph with q^{r-1}, $q \equiv 1 \pmod 4$, vertices and whose vertex set is a set of q^{r-1} column vectors $\left(1, a_{1j}, \ldots, a_{(r-1)j}\right)^{\mathbf{T}} \in \mathbb{F}_q^r$, $1 \leq j \leq q^{r-1}$ such that no two vectors are proportional. A set of r vertices S is a face or hyperedge of the r-graph if the determinant of the $r \times r$ matrix defined by S is a quadratic residue. For this to make sense we need $q \equiv 1 \pmod 4$ as before. Any collection of r vertices that is not a face we shall call a non-face. Any non-face whose vertex vectors are dependent we shall call dependent, and whose vertex vectors are independent we shall call independent. We have the following theorems:

Theorem 49 *Given two faces or two independent non-faces there is an automorphism of P_q^r taking one to the other, given by $\varphi : \mathbb{F}_q^r \to \mathbb{F}_q^r$, $\varphi(\mathbf{x}) = \mathbf{A}\mathbf{x}$, with $\mathbf{A} = (a_{ij})$ and $a_{11} = 1$, $a_{1i} = 0$, $2 \leq i \leq r$.*

This is analogous to (8.2).

Proof. Let $\mathbf{F}_1$ and $\mathbf{F}_2$ be $r \times r$ matrices consisting of column vectors from two faces or two independent non-faces. Then we wish to find a matrix $\mathbf{A} = (a_{ij})$ of the required type with $\mathbf{AF}_1 = \mathbf{F}_2$. Since $\mathbf{F}_1$ and $\mathbf{F}_2$ are both non-singular such a matrix does exist, and is equal to $\mathbf{F}_2\mathbf{F}_1^{-1}$. Also, $\mathbf{A}$ is unique and its top row only determines the top row of $\mathbf{F}_2$, which consists of all 1's. Since

$$a_{11} = 1, a_{1i} = 0, \ 2 \leq i \leq r \tag{8.3}$$

is a valid solution to this, and $\mathbf{A}$ is unique, (8.3) must hold, and $\mathbf{A}$ is of the correct form. Also as $\mathbf{F}_1$ and $\mathbf{F}_2$ represent 2 faces or two independent non-faces $\chi(\det A) = \chi(\det \mathbf{F}_2)/\chi(\det \mathbf{F}_1) = 1$, so if $\varphi : \mathbb{F}_q^r \to \mathbb{F}_q^r$, $\varphi(\mathbf{x}) = \mathbf{Ax}$, then φ is an automorpism of P_q^r. Hence the result holds.

Theorem 50 *P_q^r is regular and every face (independent non-face) of P_q^r has exactly the same number of adjacent faces and the same number of non-faces as every other face (independent non-face).*

Proof. This follows from Theorem 49 since for any two faces or independent non-faces there is an automorphism between them which obviously preserves numbers of adjacent faces and non-faces.

Chapter 9

Subgraphs of the Paley Graph

9.1 Introduction

Bollobas [11], p 317, calls a graph r-full if it contains every graph of order r as an induced subgraph. His theorem 11 shows that if $r \geq 2$, and $q \equiv 1 \pmod 4$ is a prime power satisfying

$$q > \left\{(r-2)2^{r-1}+1\right\} q^{1/2} + r2^{r-1}.$$

Then the graph P_q is $(r+1)$-full. In particular, if $q > r^2 2^{2r-2}$ then the condition holds.

We shall now see how some of these theorems can be improved and extended.

9.2 The subgraphs of P_q

Theorem 51 *Let $q = p^m$ where p is a prime, $q \equiv 1 \pmod 4$, $m \geq 1$. Then if conjecture 14 is true and s satisfies*

$$q > s^2 2^{s+2}$$

P_q contains every graph on s vertices as a subgraph.

Proof. This follows directly from theorem 38. ■

This is a considerable improvement on the result of Bollobas. This seems to be because we use the more powerful generalised Hasse-Weil estimate whereas Bollobas uses the one variable Hasse-Weil theorem.

Theorem 52 *Let $q = p^m$ where p is a prime, $q \equiv 1 \pmod{k}$, k odd, $q \equiv 1 \pmod{2k}$, k even, $m \geq 1$, $k \geq 3$. Then if conjecture 14 is true and s satisfies*

$$q > 4s^2 k^{s+1}$$

P_q^k contains every c-graph on s vertices as a subc-graph.

Proof. This follows from theorem 38. ■

Thus we have a sub c-graph very close to the expected size.

9.2.1 The clique number

The concept of r-fullness is closely connected to the clique number of a graph. This number, $cl(G)$ is defined as the size of the largest clique or complete subgraph of G. Obviously if G is r-full then we must have $cl(G) \geq r$.

The actual clique number of the Paley graph P_q is unknown if q is prime, though if q is a perfect square the clique number is $\sqrt{q}$. For P_q the clique number is at least as large as the smallest non-residue s, since then $\{1, 2, \ldots, s-1\}$ form the vertex set of a clique. Montgomery [47] proved, assuming the Riemann Hypothesis for all L-functions of real characters, that this has value sometimes at least $\epsilon \ln n \ln\ln\ln n$ for some $\epsilon > 0$. The results of [10], [13] and [36] or Bollobas' result show that $cl(P_q) > \frac{1}{2}\ln_2 q$. Thomason [59] mentions the possibility of obtaining $cl(P_q) > \ln_2 q$ by replacing Weil's estimates by those of Deligne, but says that "...this would be a formidable undertaking". This is what we are attempting to do in this section. In fact we shall demonstrate the result assuming conjecture 14, which is hopefully a consequence, albeit not an easy one, of Deligne's great work.

9.3 Difference sets

We shall apply theorem 38 to prove some estimates for squares and non-squares in difference sets in a finite field $\mathbb{F}_q$.

A residue difference set in $\mathbb{F}_q$ is a set $\{a_1, \ldots, a_k\}$, $a_i \in \mathbb{F}_q^*$, $q \equiv 1 \bmod 4$ such that

1. $\chi(a_i) = 1$, $1 \leq i \leq k$,

2. $\chi(a_i - a_j) = 1, 1 \leq i < j \leq k$

where χ is a multiplicative character of order 2. If we denote the maximal cardinality of a residue difference set in $\mathbb{F}_q$ by m_q, for the case of q prime, Buell and Williams [16] proved that $m_q > \frac{1}{2} \ln p$ for all p. Let us consider the graph G on $n+1$ vertices formed by taking the complete graph on n vertices and adding a vertex x which is connected to all the n vertices. By our result in chapter 9 we know that G is contained in P_q for all $q \geq (n+1)^2 2^{n+3}$. Thus we have a set of $n+1$ values $x, b_1, \ldots, b_n \in \mathbb{F}_q$ s.t

1. $\chi(b_i - x) = 1, 1 \leq i \leq k,$

2. $\chi(b_i - b_j) = 1, 1 \leq i < j \leq k$

If we now take a new set, $a_i = b_i - x$ then a_i is a difference set in $\mathbb{F}_q$. Thus we have a set with n members for all n with $q \geq (n+1)^2 2^{n+3}$. This gives us $m_q > \frac{c \ln q}{\ln 2}$ where $c \to 1$ as $q \to \infty$.

Various extensions of the residue difference set can be defined. Following Fabrykowski [32] we take $R_1(q)$, $R_2(q)$, $R_{12}(q)$ $(= m_q)$ to be the maximum cardinality of a set satisfying conditions 1, 2 and both 1 and 2 respectively. Then it is easy to see that we may employ the same method as before to prove that $R_2(q) > \frac{c \ln q}{\ln 2}$ where $c \to 1$ as $q \to \infty$. In fact these same methods can be used for the conditions

1. $\chi(a_i) = -1, 1 \leq i \leq k,$

2. $\chi(a_i - a_j) = -1, 1 \leq i < j \leq k$

or any reasonable combination of them. For p prime Buell and Williams prove that $m_p > \frac{\ln p}{2}$ and Fabrykowski proves the stronger result that $m_p = R_{12}(p) > \frac{\ln p}{\ln 4}$, $p \geq 29$.

9.4 A bound for q

We shall now prove theorem 38 from chapter 7 assuming conjecture 14:

Theorem 53 *38 Let c_{ij} be an arbitrary colouring of the complete graph on n vertices. If conjecture 14 is true then there is an equation of degree k which corresponds to this graph if*

$$q > 4n^2k^{n+1}, \qquad k \geq 3 \tag{9.1}$$

$$q > n^2 2^{n+2}, \qquad k = 2. \tag{9.2}$$

Let us first take an arbitrary colouring. Let c_{ij} be the colour of edge $i-j$ on the complete graph of n vertices. Thus for the colouring to be realised by some equation we must find $a_1, \ldots, a_n$, such that

$$a_i - a_j \in A_{c_{ij}} \qquad 1 \leq i < j \leq n,$$

and this in turn amounts to finding $a_1, \ldots, a_n$ such that

$$\frac{a_i - a_j}{Q^{c_{ij}}} \in R \qquad 1 \leq i < j \leq n, \tag{9.3}$$

with $A_{c_{ij}}$ and R defined as in Chapter 7.

We first introduce and prove two fundamental lemmas:

Lemma 54 *Let χ be a non-principal character of $\mathbb{F}_q$ of order k.*

Let $a \in \mathbb{F}_q^*$, then

$$\sum_{r=1}^{k} \chi(a)^r = \begin{cases} k & \text{if} \quad a \in R \\ 0 & \text{if} \quad a \notin R. \end{cases}$$

Proof. If $a \in R$, then $a = x^k$ for some $x \in \mathbb{F}_q^*$ and $\chi(a) = 1$ because χ is of order k. Hence $\sum_{r=1}^{k} \chi(a)^r = k$. If however $a \notin R$, then $\chi(a) \neq 1$ and

$$\sum_{r=1}^{k} \chi(a)^r = \frac{\chi(a)^{k+1} - \chi(a)}{\chi(a) - 1} = 0$$

since $\chi(a)^{k+1} = \chi(a)$, again because χ is of order k. ■

In order to complete our result we need to give an estimate on the modulus of sums like $f = \sum_{a_1=1}^{q} \cdots \sum_{a_n=1}^{q} \chi\left[\prod_{i<j}(a_i - a_j)^{r_{ij}}\right]$. The problem here lies in determining whether our conjecture 14 may be applied or whether the sum needs to be reduced further before it can be.

If f contains d variables we associate each sum with a graph G_f on d vertices given by

$$\text{vertex } i \text{ is connected to vertex } j \text{ if } r_{ij} \neq 0.$$

The crucial problem is to determine the rank of the sum matrix from the structure of the graph. We can then use use combinatorial estimates to sum over the subgraphs of the graph on n vertices.

We note that G_f is connected if and only if f is connected. Also the connectivity of f is equal to the connectivity of G_f.

Lemma 55 *Let χ be a multiplicative character of $\mathbb{F}_q$ of order k. Let r_{ij}, $1 \leq i < j \leq n$ be a set of integers with $1 \leq r_{ij} \leq k$. Also, let us assume that the polynomial $F = \prod_{i \neq j}(a_i - a_j)^{r_{ij}}$ depends on exactly v of the $a_i's$, $v \geq 2$, and that exactly e of the r_{ij} are not equal to k. Let $r_1, \ldots, r_c$ be the sum of r_{ij} over each component of F and let us assume that the connectivity of F is equal to c. Then, assuming conjecture 14, we have in the case $r_i \equiv 0 \pmod{k}$, $1 \leq i \leq c$,*

$$\left| \sum_{a_1=1}^{q} \cdots \sum_{a_n=1}^{q} \chi \left[\prod_{i<j} (a_i - a_j)^{r_{ij}} \right] \right| \leq \left(\frac{e-c}{v-2c} \right)^{v-2c} q^{\frac{n-v+2c}{2}}$$

and, in the case when some $r_i \neq 0 \pmod{k}$

$$\left| \sum_{a_1=1}^{q} \cdots \sum_{a_n=1}^{q} \chi \left[\prod_{i<j} (a_i - a_j)^{r_{ij}} \right] \right| = 0$$

We note that $\prod_{i<j}(a_i - a_j)^{r_{ij}}$ will not depend on a_i, for example, only if $r_{ij} = k$, for all $1 \leq j \leq n$.

Proof. Let the c components of F have $e_1, \ldots, e_c$ edges respectively and $v_1, \ldots, v_c$ vertices. We note that $e_1 + \cdots + e_c = e$ and $v_1 + \cdots + v_c = v$. Also let $r_1, \ldots, r_c$ be the sum of r_{ij} over each component. Then to estimate the character sum we need only estimate the sums for each component and multiply the results. Let F_i be the i-th component of F. Now the rank of the homogeneous form F is equal to $v_i - \eta_i$ where η_i is the dimension of the solution set of the equations $\{a_i - a_j = 0 : r_{ij} \neq k\}$. Since F_i is connected, this solution set has dimension 1. Hence rank $F_i = n - 1$.

We may then apply (3.5) with $t = e_i$, $\rho = 1$, $n = v_i$ giving

$$\left|\sum \chi(F_i)\right| \begin{array}{l} = \\ \leq \end{array} \begin{cases} 0 & if \quad r_i \neq 0 \pmod{k} \\ \left(\frac{e_i-1}{v_i-2}\right)^{v_i-2} q^{\frac{v_i+2}{2}} & if \quad r_i \equiv 0 \pmod{k} \end{cases}.$$

If $r_i = 0 \pmod{k}$, $1 \leq i \leq c$, then multiplying these estimates gives,

$$\begin{aligned} \left|\sum_{a_1=1}^{q} \cdots \sum_{a_n=1}^{q} \chi\left[\prod_{i<j}(a_i - a_j)^{r_{ij}}\right]\right| &\leq q^{n-v} \prod_{i=1}^{c} \left(\frac{e_i-1}{v_i-2}\right)^{v_i-2} q^{\frac{v_i+2}{2}} \\ &= q^{\frac{2n-v+2c}{2}} \prod_{i=1}^{c} \left(\frac{e_i-1}{v_i-2}\right)^{v_i-2} \\ &\leq q^{\frac{2n-v+2c}{2}} \left(\frac{e-c}{v-2c}\right)^{v-2c}, \end{aligned}$$

by inequality (3.4), where the q^{n-v} arises from summing over the additional $n - v$ variables.

If $r_u \neq 0 \pmod{k}$ for some $1 \leq u \leq c$ then we have

$$\sum \chi(F_u) = 0$$

by (3.5) and hence

$$\left|\sum_{a_1=1}^{q} \cdots \sum_{a_n=1}^{q} \chi\left[\prod_{i<j}(a_i - a_j)^{r_{ij}}\right]\right| = \prod_{i=1}^{c} \left[\sum \chi(F_i)\right] = 0.$$

■

Corollary 56 *If $k = 2$ then since $r_i = e_i$, the number of edges, e_i in each component must be even for the sum in lemma 55 to be non-zero.*

Proof. This follows from the above lemma since if the number of edges , e_i in a component is odd, and $k = 2$, then $e_i \neq 0 \pmod{k}$ and the sum must be zero by lemma 55. ■

9.5 Preliminaries to theorem 38

We first note two inequalities that we will use often in what follows:

If $x, n \neq 0$ and $n \in \mathbb{Z}$

$$e^x > 1 + x, \tag{9.4}$$

$$e^x > \left(1 + \frac{x}{n}\right)^n. \tag{9.5}$$

If x is positive and not equal to 1, then

$$\begin{aligned} x^r - 1 &> r(x-1) \qquad (r > 1), \\ x^r - 1 &< r(x-1) \qquad (0 < r < 1). \end{aligned} \tag{9.6}$$

Lemma 57 *Let a_i, n, r, n be positive integers with $a_1 + \cdots + a_n = r$, $a_i \geq b \geq 3$ and $n \geq 2$. Then*

$$\sum_{i=1}^{n} \binom{a_i}{2} \leq \binom{r - 2(n-1)}{2}.$$

Proof.

$$\begin{aligned} \binom{r}{2} - \sum_{i=1}^{n} \binom{a_i}{2} &= \frac{1}{2}\left[\left(\sum a_i\right)^2 - \sum a_i - \sum a_i^2 + \sum a_i\right] \\ &= \sum_{i>j} a_i a_j. \end{aligned} \tag{9.7}$$

Now

$$\begin{aligned} \binom{r}{2} - \binom{r - 2(n-1)}{2} &= \frac{1}{2}[r(r-1) - (r - 2(n-1))(r - 2(n-1) - 1)] \\ &= \frac{1}{2}[2(2n - 2 + 1 - 1)r - 2(n-1)\,(2(n-1) + 1))] \\ &= 2(n-1)r - \binom{2n-1}{2}. \end{aligned} \tag{9.8}$$

Also, because $a_i \geq 3$, $(a_i - 3)(a_j - 3) \geq 0$. Writing this as $a_i a_j \geq 3a_i + 3a_j - 9$ and summing over all $1 \leq j < i \leq n$ gives

$$\begin{aligned} \sum_{i>j} a_i a_j &\geq 3(n-1)\sum_i a_i - 9\binom{n}{2} \\ &= 3(n-1)r - \frac{9n(n-1)}{2}. \end{aligned} \tag{9.9}$$

This gives

$$\begin{aligned}\binom{r-2(n-1)}{2}-\sum_{i=1}^{n}\binom{a_i}{2} &= \left(\binom{r}{2}-\sum_{i=1}^{n}\binom{a_i}{2}\right)-\left(\binom{r}{2}-\binom{r-2(n-1)}{2}\right)\\ &= \sum_{i>j}a_ia_j-2(n-1)r+\binom{2n-1}{2}\\ &\geq 3(n-1)r-\frac{9n(n-1)}{2}-2(n-1)r+\binom{2n-1}{2}\\ &= (n-1)\left(r-\frac{(5n+2)}{2}\right)\end{aligned}$$

by (9.7), (9.8) and (9.9). $3n \leq r$ implies that $\left(r-\frac{(5n+2)}{2}\right) \geq 0$ for $n \geq 2$ giving

$$\binom{r-2(n-1)}{2} \geq \sum_{i=1}^{n}\binom{a_i}{2}.$$

Lemma 58

$$\sum_{\mathbf{x}}\chi(x_1-x_2)^r(x_2-x_3)^s(x_3-x_1)^t = 0$$

if $r+s+t \not\equiv 0 \bmod k$. *This follows from lemma 55.*

Lemma 59 *Let* $b(n,k) = \frac{\binom{q}{n}n!}{q^n}$. *Then if* $q \geq n^2 2^{n+2}$ *or* $q \geq 4n^2k^{n+1}$ *we have* $b(n,k) \geq .96$ *for* $n \geq 3$.

Proof. If $q \geq n^2 2^{n+2}$, then

$$\begin{aligned}b(n,k) &= \prod_{r=0}^{n-1}\left(1-\frac{r}{q}\right) \geq \prod_{r=0}^{n-1}\left(1-\frac{r}{n^2 2^{n+2}}\right) \geq \prod_{r=0}^{n-1}\left(1-\frac{n}{n^2 2^{n+2}}\right)\\ &= \prod_{r=0}^{n-1}\left(1-\frac{1}{n2^{n+2}}\right) = \left(1-\frac{1}{n2^{n+2}}\right)^n\\ &\geq 1-\frac{1}{2^{n+2}}\end{aligned}$$

by inequality (9.6).

By a similar argument, if $q \geq 4n^2k^{n+1}$ we have $b(n,k) \geq 1-\frac{1}{4k^{n+1}}$.

Since $1-\frac{1}{4k^{n+1}} \geq 1-\frac{1}{2^{n+2}}$, we have $b(n,k) \geq 1-\frac{1}{2^{n+2}} \geq .96$ for $n \geq 3$.

Lemma 60 *Let* $u(n,v) = \dfrac{n-v+1}{n+1}\left(\dfrac{2(n+1)^2}{n^2}\right)^{\frac{v}{4}}$ *and* $s(n,v) = \dfrac{n-v+1}{n+1}\left(\dfrac{k(n+1)^2}{n^2}\right)^{\frac{v}{6}}$. *Then for fixed* n, u *and* s *take their minimum values for* $v = n$ *or* $v = 3$.

Proof. Partially differentiating both functions with respect to v shows u and s possess only one local maximum between $v = 3$ and $v = n$. Therefore the minimum values of u and s occur at the endpoints of the interval $3 \leq v \leq n$. ■

9.5.1 Properties of $r(v,c,n)$ and $r'(v,c,n)$

The following theorems are concerned with properties of $r(v,c,n)$ and $r'(v,c,n)$. These functions are defined on page 104 in the proof of the main theorem. We repeat the definitions here for convenience:

$$r(v,c,n) = \binom{n}{v}\left(\frac{\binom{v-2c+2}{2}-c}{v-2c}\right)^{v-2c} 2^{\binom{v-2c+2}{2}}\left(n^2 2^{n+2}\right)^{\frac{-v+2c}{2}}$$

$$r'(v,c,n) = \binom{n}{v}\left(\frac{\binom{v-2c+2}{2}}{v-2c}\right)^{v-2c} 2^{\binom{v-2c+2}{2}}\left(n^2 2^{n+2}\right)^{\frac{-v+2c}{2}}.$$

Lemma 61 $\dfrac{r(v,c,n)}{r(v,c,n+1)} \geq \dfrac{n-v+1}{n+1}\left(\dfrac{2(n+1)^2}{n^2}\right)^{\frac{v}{4}}$.

Proof.

$$\frac{r(v,c,n)}{r(v,c,n+1)} = \frac{\binom{n}{v}\left(n^2 2^{n+2}\right)^{\frac{-v+2c}{2}}}{\binom{n+1}{v}\left((n+1)^2 2^{n+3}\right)^{\frac{-v+2c}{2}}} = \frac{n-v+1}{n+1}\left(\frac{n^2}{2(n+1)^2}\right)^{\frac{-v+2c}{2}}$$

$$= \frac{n-v+1}{n+1}\left(\frac{2(n+1)^2}{n^2}\right)^{\frac{v-2c}{2}} \geq \frac{n-v+1}{n+1}\left(\frac{2(n+1)^2}{n^2}\right)^{\frac{v-2\left\lfloor\frac{v}{4}\right\rfloor}{2}}$$

$$\geq \frac{n-v+1}{n+1}\left(\frac{2(n+1)^2}{n^2}\right)^{\frac{v}{4}}.$$

■

Lemma 62 $\dfrac{r'(n,c,n)}{r'(n+1,c,n+1)} \geq \dfrac{3}{2}e^{-1}2^{c+\frac{1}{2}}\dfrac{n-2c}{(n-2c+1)} \geq \dfrac{9}{7}e^{-1}2^{1+\frac{1}{2}}$ *if* $n \geq 13$.

Proof.

$$\frac{r'(n,c,n)}{r'(n+1,c,n+1)} = \frac{\left(\frac{\binom{n-2c+2}{2}}{n-2c}\right)^{n-2c} 2^{\frac{(n-2c+2)(n-2c+1)}{2}} \left((n)^2 2^{n+2}\right)^{\frac{-n+2c}{2}}}{\left(\frac{\binom{n-2c+3}{2}}{n-2c+1}\right)^{n-2c+1} 2^{\frac{(n-2c+3)(n-2c+2)}{2}} \left((n+1)^2 2^{n+3}\right)^{\frac{-n+2c-1}{2}}}.$$

Letting $u = n - 2c$ we have,

$$\frac{\left(\frac{\binom{n-2c+2}{2}}{n-2c}\right)^{n-2c}}{\left(\frac{\binom{n-2c+3}{2}}{n-2c+1}\right)^{n-2c+1}} = \frac{\left(\frac{\binom{u+2}{2}}{u}\right)^{u}}{\left(\frac{\binom{u+3}{2}}{u+1}\right)^{u+1}} = \frac{2(u+1)^{u+1}}{(u+2)u^u} \frac{(u+1)^u}{(u+3)^{u+1}}$$

$$= 2\left(\frac{u+1}{u}\right)^{u+1} \frac{u}{u+2} \left(\frac{u+1}{u+3}\right)^{u+1} \frac{1}{u+1}$$

$$\geq 2ee^{-2} \frac{u}{(u+1)(u+2)}$$

$$= 2e^{-1} \frac{u}{(u+1)(u+2)}, \text{ since it is well known that}$$

$$\left(1+\frac{1}{u}\right)^{u+1} > e$$

and also

$$e^2 > \left(1+\frac{2}{n+1}\right)^{n+1}$$

from inequality (9.5).

Also,

$$\frac{2^{\frac{(n-2c+2)(n-2c+1)}{2}} \left((n)^2 2^{n+2}\right)^{\frac{-n+2c}{2}}}{2^{\frac{(n-2c+3)(n-2c+2)}{2}} \left((n+1)^2 2^{n+3}\right)^{\frac{-n+2c-1}{2}}} = 2^{-(n-2c+2)} \left(\frac{(n)^2 2^{n+2}}{(n+1)^2 2^{n+3}}\right)^{\frac{-n+2c}{2}} \left((n+1)^2 2^{n+3}\right)^{\frac{1}{2}}$$

$$= \left(\frac{n}{n+1}\right)^{-n+2c} (n+1) 2^{c-\frac{1}{2}}$$

$$\geq \left(1+\frac{1}{n}\right)^{\frac{n}{2}} 2^{c-\frac{1}{2}} (n+1)$$

$$\geq \frac{3}{2} 2^{c-\frac{1}{2}} (n+1) \text{ by inequality (9.6).}$$

So, $\frac{r'(n,c,n)}{r'(n+1,c,n+1)} \geq \frac{3}{2} 2^{c-\frac{1}{2}} (n+1) 2e^{-1} \frac{u}{(u+1)(u+2)}$

$$= \frac{3}{2} e^{-1} 2^{c+\frac{1}{2}} (n+1) \frac{u}{(u+1)(u+2)}$$

$$= \frac{3}{2} e^{-1} 2^{c+\frac{1}{2}} (n+1) \frac{n-2c}{(n-2c+1)(n-2c+2)}$$

$$\geq \frac{3}{2} e^{-1} 2^{c+\frac{1}{2}} \frac{n-2c}{(n-2c+1)}.$$

If $n \geq 13$ then $n - 2c \geq n - 2\frac{n}{4} = \frac{n}{2} \geq 6$.

Hence $(n+1)\dfrac{n-2c}{(n-2c+1)(n-2c+2)} \geq \dfrac{6}{7}$. Thus $\dfrac{r(n,c,n)}{r(n+1,c,n+1)} \geq \dfrac{9}{7}e^{-1}2^{c+\frac{1}{2}}$ ■

Lemma 63 $r'(n+1, \dfrac{n+1}{4}, n+1) = \left(\frac{1}{4} + \dfrac{3}{2(n+1)} + \dfrac{2}{(n+1)^2}\right)^{\frac{n+1}{2}} 2^{-\frac{1}{8}n^2+\frac{9}{8}}$ *and is a decreasing function for* $n \geq 4$.

Proof.

$$r'(n, \frac{n}{4}, n) = \left(\frac{\binom{n-2\frac{n}{4}+2}{2}}{n-2\frac{n}{4}}\right)^{n-2\frac{n}{4}} 2^{\frac{(n-2\frac{n}{4}+2)(n-2\frac{n}{4}+1)}{2}} \left(n^2 2^{n+2}\right)^{\frac{-n+2\frac{n}{4}}{2}}$$

$$= \left(\frac{\binom{n-2\left(\frac{n}{4}\right)+2}{2}}{n\left(n-2\left(\frac{n}{4}\right)\right)}\right)^{n-2\left(\frac{n}{4}\right)} 2^{\frac{(n-2\left(\frac{n}{4}\right)+2)(n-2\left(\frac{n}{4}\right)+1)-(n+2)\left(n-2\left(\frac{n}{4}\right)\right)}{2}}$$

$$= \left(\frac{1}{4} + \frac{3}{2n} + \frac{2}{n^2}\right)^{\frac{n}{2}} 2^{-\frac{1}{8}(n+2)(n-4)}.$$

Obviously, since $\dfrac{1}{4} + \dfrac{3}{2(n+1)} + \dfrac{2}{(n+1)^2} \leq \dfrac{3}{4} < 1$ for $n \geq 4$, and $2^{-\frac{1}{8}n^2+\frac{9}{8}}$ is decreasing, $r'(n+1, \frac{n+1}{4}, n+1)$ is a decreasing function for $n \geq 4$. ■

9.5.2 Properties of $f(v,c,n)$ and $f'(v,c,n)$ for $k > 2$

The following theorems are concerned with properties of $f(v,c,n)$ and $f'(v,c,n)$. These functions are defined on page 107 in the proof of the main theorem. We repeat the definitions here for convenience:

$$f(v,c,n) = (k-1)^{-c}\binom{n}{v}k^{\binom{v-2c+2}{2}}\left(4n^2k^{n+1}\right)^{\frac{-v+2c}{2}}\left(\frac{\binom{v-2c+2}{2}-c}{v-2c}\right)^{v-2c}$$

$$f'(v,c,n) = (k-1)^{-c}\binom{n}{v}k^{\binom{v-2c+2}{2}}\left(4n^2k^{n+1}\right)^{\frac{-v+2c}{2}}\left(\frac{\binom{v-2c+2}{2}}{v-2c}\right)^{v-2c}.$$

Lemma 64 $\dfrac{f(v,c,n)}{f(v,c,n+1)} \geq \dfrac{n-v+1}{n+1}\left(\dfrac{k(n+1)^2}{n^2}\right)^{\frac{v}{6}}$.

Proof. $\dfrac{f(v,c,n)}{f(v,c,n+1)} = \dfrac{\binom{n}{v}\left(4n^2k^{n+1}\right)^{\frac{-v+2c}{2}}}{\binom{n+1}{v}\left(4(n+1)^2k^{n+2}\right)^{\frac{-v+2c}{2}}} = \dfrac{n-v+1}{n+1}\left(\dfrac{n^2}{k(n+1)^2}\right)^{\frac{-v+2c}{2}}$

$$= \frac{n-v+1}{n+1}\left(\frac{k(n+1)^2}{n^2}\right)^{\frac{v-2c}{2}}$$

$$\geq \frac{n-v+1}{n+1}\left(\frac{k(n+1)^2}{n^2}\right)^{\frac{v}{6}}. \blacksquare$$

Lemma 65 $\dfrac{f'(n,c,n)}{f'(n+1,c,n+1)} \geq 6k^{c-1}e^{-1}\dfrac{n-2c}{n-2c+1} \geq (3e^{-1})$ *if* $n \geq 4$ *and* $\geq \dfrac{10}{3}e^{-1}$ *if* $n \geq 5$.

$$\frac{f'(n,c,n)}{f'(n+1,c,n+1)} = \frac{k^{\binom{n-2c+2}{2}}\left(4n^2k^{n+1}\right)^{\frac{-n+2c}{2}}\left(\frac{\binom{n-2c+2}{2}}{n-2c}\right)^{n-2c}}{k^{\binom{n-2c+3}{2}}\left(4(n+1)^2k^{n+2}\right)^{\frac{-n+2c-1}{2}}\left(\frac{\binom{n-2c+3}{2}}{n-2c+1}\right)^{n-2c+1}}.$$

Letting $u = n-2c$ we have,

$$\frac{\left(\frac{\binom{n-2c+2}{2}}{n-2c}\right)^{n-2c}}{\left(\frac{\binom{n-2c+3}{2}}{n-2c+1}\right)^{n-2c+1}} = \frac{\left(\frac{\binom{u+2}{2}}{u}\right)^{u}}{\left(\frac{\binom{u+3}{2}}{u+1}\right)^{u+1}} = \frac{2(u+1)^{u+1}}{(u+2)u^u}\frac{(u+1)^u}{(u+3)^{u+1}}$$

$$= 2\left(\frac{u+1}{u}\right)^{u+1}\frac{u}{u+2}\left(\frac{u+1}{u+3}\right)^{u+1}\frac{1}{u+1}$$

$$\geq 2ee^{-2}\frac{u}{(u+1)(u+2)}$$

$$= 2e^{-1}\frac{u}{(u+1)(u+2)} \text{ as in lemma 62.}$$

Also,

$$\frac{k^{\binom{n-2c+2}{2}}\left(4n^2k^{n+1}\right)^{\frac{-n+2c}{2}}}{k^{\binom{n-2c+3}{2}}\left(4(n+1)^2k^{n+2}\right)^{\frac{-n+2c-1}{2}}} = \frac{k^{\frac{(n-2c+2)(n-2c+1)}{2}}}{k^{\frac{(n-2c+3)(n-2c+2)}{2}}}\frac{\left(4n^2k^{n+1}\right)^{\frac{-n+2c}{2}}}{\left(4(n+1)^2k^{n+2}\right)^{\frac{-n+2c-1}{2}}}$$

$$= k^{-(n-2c+2)}\left(\frac{n^2k^{n+1}}{(n+1)^2k^{n+2}}\right)^{\frac{-n+2c}{2}}\left(4(n+1)^2k^{n+2}\right)^{\frac{1}{2}}$$

$$= 2k^{c-1}\left(\frac{n}{n+1}\right)^{-n+2c}(n+1)$$

$$\geq 2k^{c-1}\left(1+\frac{1}{n}\right)^{\frac{n}{3}}(n+1)$$

$$\geq \frac{8}{3}k^{c-1}(n+1) \text{ by inequality (9.6).}$$

Hence, $\dfrac{f'(n,c,n)}{f'(n+1,c,n+1)} \geq 2e^{-1}\dfrac{u}{(u+1)(u+2)}\dfrac{8}{3}k^{c-1}(n+1) \geq \dfrac{16}{3}k^{c-1}e^{-1}\dfrac{n-2c}{n-2c+1}$.

Now if $n \geq 4$, $n-2c \geq \dfrac{4}{3}$, so

$$\frac{f'(n,c,n)}{f'(n+1,c,n+1)} \geq \frac{4}{7}\times\frac{16}{3}k^{c-1}e^{-1} = \frac{64}{21}k^{c-1}e^{-1} \geq 3k^{c-1}e^{-1} \geq 3e^{-1}$$

If $n \geq 5$, $n-2c \geq \dfrac{5}{3}$, so

$$\frac{f'(n,c,n)}{f'(n+1,c,n+1)} \geq \frac{5}{8}\times\frac{16}{3}k^{c-1}e^{-1} = \frac{10}{3}k^{c-1}e^{-1} \geq \frac{10}{3}e^{-1} \blacksquare$$

Lemma 66 $f'(n+1,\frac{n+1}{3},n+1)=2^{-\frac{n+1}{3}}(k-1)^{-\frac{n+1}{3}}k^{-\frac{1}{9}(n+1)^2+\frac{1}{3}(n+1)+1}\left(\frac{1}{6}+\frac{3}{2(n+1)}+\frac{3}{(n+1)^2}\right)^{\frac{n+1}{3}}$ *and* $f'(n+1,\frac{n+1}{3},n+1)$ *is a decreasing function of* k *and* n, *for* $n\geq 4$.

Proof.

$$f'(n,\frac{n}{3},n)=(k-1)^{-\frac{n}{3}}k^{\binom{n-2\frac{n}{3}+2}{2}}\left(4n^2k^{n+1}\right)^{\frac{-n+2\frac{n}{3}}{2}}\left(\frac{\binom{n-2\frac{n}{3}+2}{2}}{n-2\frac{n}{3}}\right)^{n-2\frac{n}{3}}$$

$$=\left(1+\frac{1}{k-1}\right)^{\frac{n}{3}}k^{-\frac{n}{3}}k^{\binom{n-2\frac{n}{3}+2}{2}}\left(4k^{n+1}\right)^{\frac{-n+2\frac{n}{3}}{2}}\left(\frac{\binom{n-2\frac{n}{3}+2}{2}}{n\left(n-2\frac{n}{3}\right)}\right)^{n-2\frac{n}{3}}$$

$$=\left(1+\frac{1}{k-1}\right)^{\frac{n}{3}}k^{-(\frac{n}{3}-1)((\frac{n}{3})+1)}(2)^{(-n+2(\frac{n}{3}))}\left(\frac{\binom{n-2(\frac{n}{3})+2}{2}}{n\left(n-2\left(\frac{n}{3}\right)\right)}\right)^{n-2(\frac{n}{3})}$$

This shows that the expression $f(n,\left\lfloor\frac{n}{3}\right\rfloor,n)$ is a decreasing function of k as

$$-\left(\frac{n}{3}-1\right)\left(\left(\frac{n}{3}\right)+1\right)\leq 0 \text{ for } n\geq 3.$$

Continuing we obtain

$$f(n,\left\lfloor\frac{n}{3}\right\rfloor,n)=2^{-\frac{n}{3}}(k-1)^{-\frac{n}{3}}k^{-\frac{1}{9}n^2+\frac{1}{3}n+1}\left(\frac{1}{6}+\frac{3}{2n}+\frac{3}{n^2}\right)^{\frac{n}{3}}\cdot$$

$$2^{-\frac{n+1}{3}}(k-1)^{-\frac{n+1}{3}}k^{-\frac{1}{9}(n+1)^2+\frac{1}{3}(n+1)+1}\left(\frac{1}{6}+\frac{3}{2(n+1)}+\frac{3}{(n+1)^2}\right)^{\frac{n+1}{3}}$$

If $n\geq 4$, $\frac{1}{6}+\frac{3}{2(n+1)}+\frac{3}{(n+1)^2}\leq\frac{44}{75}<1$, hence $f(n+1,\left\lfloor\frac{n+1}{3}\right\rfloor,n+1)$ is a decreasing function of n for $n\geq 4$. ■

9.6 Proof of theorem 38.

Using lemma 54 we can see that

$$\sum_{r_{ij}=1}^{k}\chi\left[\left(\frac{a_i-a_j}{Q^{c_{ij}}}\right)^{r_{ij}}\right]$$

will equal 0 if edge ij does not have colour c_{ij}, and 1 if edge ij does have colour c_{ij}. Thus we have a characteristic function for one of the edges. Hence

$$\sum_{r_{12}=1}^{k} \chi\left[\left(\frac{a_1-a_2}{Q^{c_{12}}}\right)^{r_{12}}\right] \sum_{r_{13}=1}^{k} \chi\left[\left(\frac{a_1-a_3}{Q^{c_{13}}}\right)^{r_{13}}\right] \cdots \sum_{r_{n-1n}=1}^{k} \chi\left[\left(\frac{a_{n-1}-a_n}{Q^{c_{n-1n}}}\right)^{r_{n-1n}}\right]$$

$$= \sum_{r_{12}=1}^{k} \cdots \sum_{r_{n-1n}=1}^{k} \prod_{i<j} \chi\left[\left(\frac{a_i-a_j}{Q^{c_{ij}}}\right)^{r_{ij}}\right]$$

$$= \begin{cases} 1, & \text{if each edge ij has colour } c_{ij}, \\ 0, & \text{otherwise.} \end{cases}$$

Now, letting $a_1, \ldots, a_n$ run through all possible values we see that the total number N of suitable colourings arising out of all possible colourings is given by

$$k^{\binom{n}{2}} N = \sum_{a_1=1}^{q} \cdots \sum_{a_n=1}^{q} \sum_{r_{11}=1}^{k} \cdots \sum_{r_{nn}=1}^{k} \chi\left[\prod_{i<j}\left(\frac{a_i-a_j}{Q^{c_{ij}}}\right)^{r_{ij}}\right].$$

Taking the term corresponding to $r_{ij} = k$, $1 \le i < j \le n$ to the left-hand side we obtain

$$k^{\binom{n}{2}} N - \binom{q}{n} n! = \sum_{a_1=1}^{q} \cdots \sum_{a_n=1}^{q} \sum_{r_{11}=1}^{k} \cdots \sum_{r_{nn}=1}^{k} \chi\left[\prod_{i<j}\left(\frac{a_i-a_j}{Q^{c_{ij}}}\right)^{r_{ij}}\right].$$

and hence we have a solution if

$$\sum_{a_1=1}^{q} \cdots \sum_{a_n=1}^{q} \sum_{r_{11}=1}^{k} \cdots \sum_{r_{nn}=1}^{k} \chi\left[\prod_{i<j}\left(\frac{a_i-a_j}{Q^{c_{ij}}}\right)^{r_{ij}}\right] < \binom{q}{n} n!.$$

The left-hand side is equal to

$$\sum_{r_{11}=1}^{k} \cdots \sum_{r_{nn}=1}^{k} \chi(Q^{c_{ij}})^{-r_{ij}} \sum_{a_1=1}^{q} \cdots \sum_{a_n=1}^{q} \chi\left[\prod_{i<j}(a_i-a_j)^{r_{ij}}\right].$$

In modulus this is

$$\left|\sum_{r_{11}=1}^{k} \cdots \sum_{r_{nn}=1}^{k} \chi(Q^{c_{ij}})^{-r_{ij}} \sum_{a_1=1}^{q} \cdots \sum_{a_n=1}^{q} \chi\left[\prod_{i<j}(a_i-a_j)^{r_{ij}}\right]\right|$$

$$\leq \sum_{r_{11}=1}^{k} \cdots \sum_{r_{nn}=1}^{k} \left| \sum_{a_1=1}^{q} \cdots \sum_{a_n=1}^{q} \chi \left[\prod_{i<j} (a_i - a_j)^{r_{ij}} \right] \right|$$

by the triangle inequality.

As above, to each term $\left|\sum_{a_1=1}^{q} \cdots \sum_{a_n=1}^{q} \chi \left[\prod_{i<j}(a_i - a_j)^{r_{ij}}\right]\right|$ in the above sum we associate a subgraph of the complete graph on n vertices. The number of subgraphs with exactly v vertices, c components, e edges is given by saying that for v fixed vertices and c components an upper bound on the number of possible edges is given by $\binom{v-2c+2}{2}$, using lemma 57. Thus we simply choose the e edges from these and multiply by $\binom{n}{v}$ for the choice of vertices giving $\binom{n}{v}\binom{\binom{v-2c+2}{2}}{e}$. For each such a subgraph the number of terms in the sum is given by $(k-1)^{e-c}$ as the indices in each component must sum to zero. Thus we have in total $(k-1)^{e-c}\binom{n}{v}\binom{\binom{v-2c+2}{2}}{e}$ terms. For $k \geq 3$, since each component must have ≥ 3 vertices the number of components for a graph on v vertices is at most $\lfloor \frac{v}{3} \rfloor$. By lemma 56, if $k = 2$, each component must have ≥ 4 vertices.

Hence for $k = 2$ the total sum is

$$\sum_{v=3}^{n} \sum_{c=1}^{\lfloor \frac{v}{4} \rfloor} \sum_{e=c}^{\binom{v-2c+2}{2}} (k-1)^{e-c} \binom{n}{v} \binom{\binom{v-2c+2}{2}}{e} q^{\frac{2n-v+2c}{2}} \left(\frac{e-c}{v-2c}\right)^{v-2c}.$$

For $k \geq 3$ the total sum is

$$\sum_{v=3}^{n} \sum_{c=1}^{\lfloor \frac{v}{3} \rfloor} \sum_{e=c}^{\binom{v-2c+2}{2}} (k-1)^{e-c} \binom{n}{v} \binom{\binom{v-2c+2}{2}}{e} q^{\frac{2n-v+2c}{2}} \left(\frac{e-c}{v-2c}\right)^{v-2c}.$$

9.6.1 The case $k = 2$

Taking first the case $k = 2$ we note that for the equations to have a solution we require that the expression be less then $\binom{q}{n} n!$ for $q \geq n^2 2^{n+2}$. Thus dividing by q^n and using $q \geq n^2 2^{n+2}$ we have

$$\begin{aligned} G(n) &= \sum_{v=3}^{n} \sum_{c=1}^{\lfloor \frac{v}{4} \rfloor} \sum_{e=c}^{\binom{v-2c+2}{2}} \binom{n}{v} \binom{\binom{v-2c+2}{2}}{e} \left(n^2 2^{n+2}\right)^{\frac{-v+2c}{2}} \left(\frac{e-c}{v-2c}\right)^{v-2c} \\ &\leq g(n) = \sum_{v=3}^{n} \sum_{c=1}^{\lfloor \frac{v}{4} \rfloor} \binom{n}{v} \left(\frac{\binom{v-2c+2}{2} - c}{v-2c}\right)^{v-2c} 2^{\binom{v-2c+2}{2}} \left(n^2 2^{n+2}\right)^{\frac{-v+2c}{2}} \end{aligned}$$

$$= \sum_{v=3}^{n} \sum_{c=1}^{\lfloor \frac{v}{4} \rfloor} r(v,c,n)$$

using the fact that $e \leq \binom{v-2c+2}{2}$ and the inequality

$$\sum_{r=a}^{b} \binom{N}{r} x^r \leq (1+x)^N, \qquad 0 \leq a \leq b \leq N. \tag{9.10}$$

Thus, for a solution we need $G(n)$ or $g(n) < \frac{\binom{q}{n} n!}{q^n}$ when $q \geq n^2 2^{n+2}$. By lemma 59 we know that $\frac{\binom{q}{n} n!}{q^n} \geq .96$ when $q \geq n^2 2^{n+2}$. We will show that $g(n) < .96$ for all $n \geq 3$. We define

$$\begin{aligned} r(v,c,n) &= \binom{n}{v} \left(\frac{\binom{v-2c+2}{2} - c}{v-2c} \right)^{v-2c} 2^{\binom{v-2c+2}{2}} \left(n^2 2^{n+2} \right)^{\frac{-v+2c}{2}} \\ r'(v,c,n) &= \binom{n}{v} \left(\frac{\binom{v-2c+2}{2}}{v-2c} \right)^{v-2c} 2^{\binom{v-2c+2}{2}} \left(n^2 2^{n+2} \right)^{\frac{-v+2c}{2}} \end{aligned}$$

noting that $r'(v,c,n) \geq r(v,c,n)$. We shall split the sum $g(n+1)$ into various parts:

$$\begin{aligned} g(n+1) &= \sum_{v=3}^{n+1} \sum_{c=1}^{\lfloor \frac{v}{4} \rfloor} r(v,c,n+1) = \sum_{v=3}^{n} \sum_{c=1}^{\lfloor \frac{v}{4} \rfloor} r(v,c,n+1) + \sum_{c=1}^{\lfloor \frac{n+1}{4} \rfloor} r(n+1,c,n+1) \\ &= \sum_{v=3}^{n} \sum_{c=1}^{\lfloor \frac{v}{4} \rfloor} r(v,c,n+1) + \sum_{c=1}^{\lfloor \frac{n+1}{4} \rfloor} r(n+1,c,n+1) \\ &\leq \sum_{v=3}^{n} \sum_{c=1}^{\lfloor \frac{v}{4} \rfloor} r(v,c,n+1) + \sum_{c=1}^{\lfloor \frac{n+1}{4} \rfloor} r'(n+1,c,n+1) \end{aligned}$$

Now we also define

$$d(n) = \sum_{c=1}^{\lfloor \frac{n}{4} \rfloor} r'(n,c,n)$$

which satisfies

$$d(n+1) = \sum_{c=1}^{\lfloor \frac{n+1}{4} \rfloor} r'(n+1,c,n+1)$$

$$\leq \sum_{c=1}^{\lfloor \frac{n}{4} \rfloor} r'(n+1,c,n+1) + r'(n+1,\frac{n+1}{4},n+1)$$

as we may remove the $\lfloor \rfloor$ since the last term occurs only if $\left\lfloor \frac{n+1}{4} \right\rfloor = \frac{n+1}{4}$.

Lemma 67 *Let $d(n)$, and $g(n)$ be defined as above, and*

$$\frac{r(v,c,n+1)}{r(v,c,n)} \leq a$$
$$\frac{r'(n+1,c,n+1)}{r'(n,c,n)} \leq b$$
$$r'(n+1,\frac{n+1}{4},n+1) \leq c$$

for all $n \geq N$ and $0 < a,b,c < 1$. Then if $c < e(1-a)(1-b)$, with $0 < e < 1$ and D,G are defined by $D = e(1-a)$ and $G = e$, we have ,

$$d(n) < D \Longrightarrow d(n+1) < D$$

and

$$g(n) < G \Longrightarrow g(n+1) < G$$

for $n \geq N$.

Proof. If $d(n) < D$, then

$$\begin{aligned} d(n+1) &\leq \sum_{c=1}^{\lfloor \frac{n}{4} \rfloor} r'(n+1,c,n+1) + r(n+1,\frac{n+1}{4},n+1) \\ &\leq b\sum_{c=1}^{\lfloor \frac{n}{4} \rfloor} r'(n,c,n) + c \\ &< bD + c = be(1-a) + c \\ &< be(1-a) + e(1-a)(1-b) = e(1-a) = D. \end{aligned}$$

If $g(n) < G$, then

$$\begin{aligned} g(n+1) &\leq \sum_{v=3}^{n}\sum_{c=1}^{\lfloor \frac{v}{4} \rfloor} r(v,c,n+1) + \sum_{c=1}^{\lfloor \frac{n+1}{4} \rfloor} r'(n+1,c,n+1) \\ &\leq a\sum_{v=3}^{n}\sum_{c=1}^{\lfloor \frac{v}{4} \rfloor} r(v,c,n) + D = ag(n) + D \\ &\leq aG + D = G. \end{aligned}$$

■

If $n \geq 13$, from lemmas 60,61, 62 and 63 we have,

$\frac{r(v,c,n+1)}{r(v,c,n)} \leq .91 = a$

$\frac{r'(n+1,c,n+1)}{r'(n,c,n)} \leq .75 = b$

$r(n+1, \lfloor \frac{n+1}{4} \rfloor, n+1) \leq 8.7 \times 10^{-10} = c$

We then apply lemma 67 for $N = 13$ with $e = .95$ and a, b, c defined as above.

This gives $G = .95$, $D = .95 \times (1 - .91) = .0855$.

The conditions of the lemma are satisfied as $e(1-a)(1-b) = .95 \times (1 - .91) \times (1 - .75) = .021375 > 8.7 \times 10^{-10} = c$.

We then use the explicit formulas for g and d to check that $d(13) < .085$ and $g(13) < .95$. This gives us a solution for all $n \geq 13$. We then verify that $g(n) < .96$ for $3 \leq n \leq 12$.

9.6.2 The case $k \geq 3$

For $k \geq 3$ the total sum is

$$\sum_{v=3}^{n}\sum_{c=1}^{\lfloor \frac{v}{3} \rfloor}\sum_{e=c}^{\binom{v-2c+2}{2}} (k-1)^{e-c}\binom{n}{v}\binom{\binom{v-2c+2}{2}}{e} q^{\frac{2n-v+2c}{2}} \left(\frac{e-c}{v-2c}\right)^{v-2c}.$$

For the equations to have a solution we require that the expression be less then $\binom{q}{n}n!$ for $q \geq 4n^2k^{n+1}$. Thus dividing by q^n and using $q \geq 4n^2k^{n+1}$ we have,

$$G(n) = \sum_{v=3}^{n}\sum_{c=1}^{\lfloor \frac{v}{3} \rfloor}\sum_{e=c}^{\binom{v-2c+2}{2}} (k-1)^{e-c}\binom{n}{v}\binom{\binom{v-2c+2}{2}}{e} q^{\frac{-v+2c}{2}} \left(\frac{e-c}{v-2c}\right)^{v-2c}$$

$$\leq g(n) = \sum_{v=3}^{n} \sum_{c=1}^{\lfloor \frac{v}{3} \rfloor} (k-1)^{-c} \binom{n}{v} k^{\binom{v-2c+2}{2}} \left(4n^2k^{n+1}\right)^{\frac{-v+2c}{2}} \left(\frac{\binom{v-2c+2}{2} - c}{v-2c}\right)^{v-2c}$$

$$= \sum_{v=3}^{n} \sum_{c=1}^{\lfloor \frac{v}{3} \rfloor} f(v,c,n)$$

Thus, for a solution we need $G(n)$ or $g(n) < \frac{\binom{q}{n} n!}{q^n}$ when $q \geq 4n^2k^{n+1}$. By lemma 59 we know that $\frac{\binom{q}{n} n!}{q^n} \geq .96$ when $q \geq 4n^2k^{n+1}$. We will show that $g(n) < .96$ for all $n \geq 3$. We define

$$f(v,c,n) = (k-1)^{-c} \binom{n}{v} k^{\binom{v-2c+2}{2}} \left(4n^2k^{n+1}\right)^{\frac{-v+2c}{2}} \left(\frac{\binom{v-2c+2}{2} - c}{v-2c}\right)^{v-2c}$$

$$f'(v,c,n) = (k-1)^{-c} \binom{n}{v} k^{\binom{v-2c+2}{2}} \left(4n^2k^{n+1}\right)^{\frac{-v+2c}{2}} \left(\frac{\binom{v-2c+2}{2}}{v-2c}\right)^{v-2c}$$

noting that $f'(v,c,n) \geq f(v,c,n)$. We shall split the sum $g(n+1)$ into various parts:

$$g(n+1) = \sum_{v=3}^{n+1} \sum_{c=1}^{\lfloor \frac{v}{3} \rfloor} f(v,c,n+1) = \sum_{v=3}^{n} \sum_{c=1}^{\lfloor \frac{v}{3} \rfloor} f(v,c,n+1) + \sum_{c=1}^{\lfloor \frac{n+1}{3} \rfloor} f(n+1,c,n+1)$$

$$= \sum_{v=3}^{n} \sum_{c=1}^{\lfloor \frac{v}{3} \rfloor} f(v,c,n+1) + \sum_{c=1}^{\lfloor \frac{n+1}{3} \rfloor} f(n+1,c,n+1)$$

$$\leq \sum_{v=3}^{n} \sum_{c=1}^{\lfloor \frac{v}{3} \rfloor} f(v,c,n+1) + \sum_{c=1}^{\lfloor \frac{n+1}{3} \rfloor} f'(n+1,c,n+1)$$

Now we also need to define

$$d(n) = \sum_{c=1}^{\lfloor \frac{n}{3} \rfloor} f'(n,c,n).$$

We see that $d(n)$ satisfies

$$d(n+1) = \sum_{c=1}^{\lfloor \frac{n+1}{3} \rfloor} f'(n+1,c,n+1)$$

$$= \sum_{c=1}^{\lfloor \frac{n}{3} \rfloor} f'(n+1,c,n+1) + f'(n+1,\frac{n+1}{3},n+1)$$

$$\leq \sum_{c=1}^{\lfloor \frac{n}{3} \rfloor} f'(n+1,c,n+1) + f'(n+1,\frac{n+1}{3},n+1)$$

since the last term occurs only if $\left\lfloor \frac{n+1}{3} \right\rfloor = \frac{n+1}{3}$.

Lemma 68 *Let $d(n)$, and $g(n)$ be defined as above, and*

$$\frac{f(v,c,n+1)}{r(v,c,n)} \leq a$$
$$\frac{f'(n+1,c,n+1)}{r'(n,c,n)} \leq b$$
$$f'(n+1,\frac{n+1}{3},n+1) \leq c$$

for all $n \geq N$ and $0 < a,b,c < 1$. Then if $c < e(1-a)(1-b)$, with $0 < e < 1$ and D,G are defined by $D = e(1-a)$ and $G = e$, we have,

$$d(n) < D \Longrightarrow d(n+1) < D$$

and

$$g(n) < G \Longrightarrow g(n+1) < G$$

for $n \geq N$.

Proof. See proof of lemma 67 ■

Calculations for $k \geq 10$

If $k \geq 10$, from lemmas 60,64, 65 and 66 we have,

$\frac{f(v,c,n+1)}{f(v,c,n)} \leq .8 = a$ for $n \geq 4$

$\frac{f'(n+1,c,n+1)}{f'(n,c,n)} \leq \left(3e^{-1}\right)^{-1} \leq .91 = b$ for $n \geq 4$

$f(n+1,\left\lfloor \frac{n+1}{3} \right\rfloor, n+1) \leq 2.6 \times 10^{-3} = c$

We may then apply lemma 68 with a,b,c as above and $e = .95$.

Then we have $D = .95 \times (1-.8) = .19$, $G = .95$.

The conditions of the lemma apply as

$e(1-a)(1-b) = .95 \times (1-.8) \times (1-.91) = .0171 > 2.6 \times 10^{-3} = c.$

$d(n)$ is a decreasing function of k and $d(3) < .19, d(4) < .19$ for $k = 10$.

Also $g(3) = f(3,1,3) = \left(\frac{k}{k-1}\right)\frac{1}{3} \leq .95$ and $g(4) = f(3,1,4) + f(4,1,4) < .95$. Hence the result follows from lemma 68.

Calculations for $3 \leq k \leq 9$

If $3 \leq k \leq 9$, then from lemmas 60,64, 65 and 66 we have,

$k = 9, \frac{f(v,c,n+1)}{f(v,c,n)} \leq .71 = a$ for $n \geq 5$

$k = 8, \frac{f(v,c,n+1)}{f(v,c,n)} \leq .79 = a$ for $n \geq 5$

$k = 7, \frac{f(v,c,n+1)}{f(v,c,n)} \leq .88 = a$ for $n \geq 5$

$k = 6, \frac{f(v,c,n+1)}{f(v,c,n)} \leq .86 = a$ for $n \geq 6$

$k = 5, \frac{f(v,c,n+1)}{f(v,c,n)} \leq .90 = a$ for $n \geq 7$

$k = 4, \frac{f(v,c,n+1)}{f(v,c,n)} \leq .92 = a$ for $n \geq 9$

$k = 3, \frac{f(v,c,n+1)}{f(v,c,n)} \leq .94 = a$ for $n \geq 13$

$\frac{f'(n+1,c,n+1)}{f'(n,c,n)} \leq \left(\frac{10}{3}e^{-1}\right)^{-1} = .82 = b$ for $n \geq 4$.

$f(n+1, \left\lfloor \frac{n+1}{3} \right\rfloor, n+1) \leq 5.3 \times 10^{-3}$ for $n \geq 4$, $k \geq 3$.

For all these values we have $a \leq .94$, so we again use lemma 68 with

$D = .95 \times (1-a) \geq .057$, $G = .95$.

The conditions of the lemma are satisfied as $e(1-a)(1-b) \geq .95 \times (1-.94) \times (1-.82) = .01026 > 5.3 \times 10^{-3} = c$.

We verified by direct calculation that $d(n) < .057$ for the first value of n in each range. Then we checked that the values of n not covered by the above satisfy $g(n) < .95$. This however does not work for $k = 3$ where the smaller values of $n = 3, \ldots, 7$ must be checked using $G(n)$, not $g(n)$. Hence the result follows from lemma 68.

Bibliography

[1] M. Aigner, Combinatorial Theory (Springer, 1979).

[2] O. D. Atkinson, PhD Dissertation, University of Sheffield, 1989.

[3] O. D. Atkinson, J. Brüdern and R. J. Cook, Three additive cubic equations, Acta Arithmetica (1991), 29-83.

[4] O. D. Atkinson, J. Brüdern and R. J. Cook. Simultaneous additive congruences to a large prime modulus, Mathematika 39 (1992), 1-9.

[5] O. D. Atkinson and R. J. Cook, Pairs of additive congruences to a large prime modulus, J. Australian Math. Soc. 46A (1989), 438-455.

[6] J. Ax and S. Kochen, Diophantine problems over local fields, I. Amer. J. Math. 87 (1965), 605-630.

[7] J. L. Berggren, an algebraic characterization of finite symmetric tournaments, Bull. Australian Math. Soc. 6 (1972), 53-59.

[8] B. J. Birch, Homogeneous forms of odd degree in a large number of variables, Mathematika 4 (1957), 102-105.

[9] B. J. Birch, D. J. Lewis and T. G. Murphy, Simultaneous quadratic forms, Amer. J. Math 84 (1962), 110-115.

[10] A. Blanchard, quoted by G. Giraud, Nouvelles majorations des nombres de Ramsey binaires-bicolores, C. R. Acad. Sci. Paris Sér. A 268 (1969), 5-7.

[11] B. Bollobás, Random Graphs, Academic Press, 1985.

[12] B. Bollobás, Combinatorics, Cambridge University Press, 1986.

[13] B. Bollobás and A. Thomason, Graphs which contain all small graphs, European J. Combinatorics 2 (1981), 13-15.

[14] R. Brauer, A note on systems of homogeneous algebraic equations, Bull. Amer. Math. Soc. 51 (1945), 749-755.

[15] J. Browkin, On forms over p-adic fields. Bull. Acad. Polon. Sci. Sér. Sci. Math. Astronom. Phys. 14 (1966), 489-492.

[16] D. A. Buell and K. D. Williams, Maximal residue difference sets modulo p, Proc. Amer. Math. Soc. 69 (1978), 205-209.

[17] C. Chevalley, Démonstration d'une hypothèse de M. Artin, Abh. Math. Sem. Univ. Hamburg. 11 (1935), 73-75.

[18] I. Chowla, On the number of solutions of some congruences in two variables, Proc. Nat. Acad. Sci. India Ser. A 5 (1937), 40-44.

[19] R. J. Cook, Pairs of additive congruences: cubic congruences, Mathematika 32 (1985), 286-300.

[20] R. J. Cook, Pairs of additive congruences: quintic congruences, Indian J. Pure Appl. Math. 17 (1986), 786-799.

[21] R. J. Cook, Computations for additive Diophantine equations: quintic congruences II, Computers in Mathematical Research. edited by N. M. Stephens and M. P. Thorne. pp.93-117 (Clarendon Press, Oxford, 1988).

[22] H.Davenport, Analytic Methods for Diophantine Equations and Diophantine Inequalities (Campus Publishers, Ann Arbor, 1963).

[23] H. Davenport and D. J. Lewis, Homogenous additive equations, Proc. Roy. Soc. London 274A (1963), 443-460.

[24] H. Davenport and D. J. Lewis, Cubic equations of additive type, Phil.Trans. Roy. Soc. London 261A (1966), 97-136.

[25] H. Davenport and D. J. Lewis, Simultaneous equations of additive type, Phil. Trans. Roy. Soc. London 264A (1969), 557-595.

[26] H. Davenport and D. J. Lewis, Two additive equations, Proc. Sympos. Pure Math, 12 (1976), 74-98.

[27] H. Davenport, Multiplicative Number Theory, Graduate Texts in Mathematics 74 revised by Hugh Montgomery (Springer Verlag, 1980).

[28] P. Deligne, La conjecture de Weil I, Publ Math. IHES 43 (1974), 273-307.

[29] V. B. Demyanov, Pairs of quadratic forms over a complete field with discrete norm with a finite residue class field, Izv. Akad. Nauk USSR. 20 (1956), 307-324 (Russian).

[30] B. Dwork, On the rationality of the zeta function of an algebraic variety, Amer. J. Math. 82 (1960), 631-648.

[31] F. Ellison, Three diagonal quadratic forms, Acta Arith. 23 (1973), 137-151.

[32] J. Fabrykowski, On quadratic residues and nonresidues in difference sets modulo m, Proc. Amer. Math. Soc. 122 (1994), 325-331.

[33] E. Fried, On homogeneous tournaments, in Combinatorial Theory and its applications II (ed. P. Erdos et al.), North Holland, 1970, 467-476.

[34] M. Goldberg, The group of the quadratic residue tournament, Canad. Math. Bull 13 (1970), 51-54.

[35] R. L. Graham and V. Rödl, Numbers in Ramsey Theory, Surveys in Combinatorics, ed. C. Whitehead (Cambridge University Press, Cambridge, 1987).

[36] R. L. Graham and J. H. Spencer, A constructive solution to a tournament problem, Canad. Math. Bull. 14 (1971), 45-48.

[37] J. F. Gray, Diagonal forms of prime degree (PhD thesis, University of Notre Dame, 1958).

[38] G. H. Hardy, J. E. Littlewood and G. Pólya. Inequalities (Cambridge University Press 1952).

[39] D. Hilbert and A. Hurwitz, Über die diophantische Gleichungen vom Geschlecht Null. Acta Math. 14 (1890), 217-224.

[40] N. M. Katz, An overview of Deligne's proof of the Riemann Hypothesis for varieties over finite fields, Proc. Symp. Pure Math. 28, American Math. Society, Providence, R.I., (1976), 275-305.

[41] S. Lang and A. Weil, Number of points of varieties in finite fields, Amer. J. Math. 76 (1954), 819-827.

[42] W. J. LeVeque, editor, Studies in Number Theory, MAA Studies in Mathematics 6 (1969).

[43] D. J. Lewis, Cubic homogeneous poynomials over p-adic fields. Ann. of Math. (2), 56 (1952), 473-478.

[44] D. J. Lewis, Cubic congruences. Michigan Math. J. 4 (1957), 85-95.

[45] R. Lidl and H. Niederreiter, Finite Fields, Encyclopedia of Mathematics and its applications 20 (1983).

[46] L. Low, J. Pitman and A. Wolff, Simultaneous diagonal congruences, J. Number Theory 29 (1988), 31-59.

[47] H. L. Montgomery, Topics in multiplicative number theory, Lecture Notes in Mathematics 227 Springer Verlag (1971).

[48] L. J. Mordell, On the rational solutions of the indeterminate equations of the third and fourth degrees, Proc. Camb. Philos. Soc. 21 (1922), 179-192.

[49] R.E.A.C. Paley, On orthogonal matrices, J. Math. Phys 12 (1933), 311-320.

[50] G. I Perelmutter, Estimation of a multiple sum involving the Legendre symbol, Math. Notes 18 (1975), 840-844.

[51] G. I. Perelmutter, Estimation of a multiple sum involving the Legendre symbol for a poynomial of odd degree, Math. Notes 20 (1976) 1015-1020.

[52] H. Poincaré, Sur les propriétés arithmétiques des courbes algébriques, J.Math. Pures Appl. (5), 7 (1901), 161-233.

[53] F. P. Ramsey, On a problem of formal logic, Proc. London Math. Soc. (2) 30, 264-286.

[54] W. M. Schmidt, Equations over Finite Fields, An Elementary Approach, Lecture Notes in Mathematics 536 Springer (1976).

[55] W. M. Schmidt, The solubility of certain p-adic equations, J. Number Theory 19 (1984), 63-80.

[56] C. L. Siegel, Über einige Anwendungen diophantischer Approximationen, Abh. Preuss. Akad Wiss Phys. Mat. Kl. No. 1 (1929).

[57] E. Stevenson, The Artin conjecture for three diagonal cubic forms, J. Number Theory 14 (1982), 374-390.

[58] G. Terjanian, Un contre-exemple à une conjecture d'Artin, C. R. Acad. Sci. Paris, Sér. A-B 262 (1966), A 612.

[59] A. Thomason, Random Graphs, strongly regular graphs and pseudo-random graphs, Surveys of Combinatorics 1987, London Mathematical Society Lecture Note Series 123, ed. C. Whitehead (Cambridge University Press, Cambridge), 173-196.

[60] A. Thue, Über annäherungswerte algebraischer Zahlen, J. Reine Angew. Math. 135 (1909), 284-305.

[61] R. C. Vaughan, The Hardy-Littlewood method, Cambridge Tracts in Mathematics No. 80, Cambridge University Press, 1981.

[62] E. Waring, Meditationes algebraicae (1770), 204-205.

[63] A. Weil, L'arithmétique sur les courbes algébriques, Acta Math. 52 (1928), 281-315.

[64] A. Weil, Number of solutions of equations in finite fields, Bull A.M.S 55 (1949), 497-508.