BLOCK DESIGNS, PERMUTATION GROUPS AND PRIME VALUES OF POLYNOMIALS

GARETH A. JONES AND ALEXANDER K. ZVONKIN

Abstract. A recent construction by Amarra, Devillers and Praeger of block designs with specific parameters and large symmetry groups depends on certain quadratic polynomials, with integer coefficients, taking prime power values. Similarly, a recent construction by Hujdurović, Kutnar, Kuzma, Marušič, Miklavič and Orel of permutation groups with specific intersection densities depends on certain cyclotomic polynomials taking prime values. The Bunyakovsky Conjecture, if true, would imply that each of these polynomials takes infinitely many prime values, giving infinite families of block designs and permutation groups with the required properties. We have found large numbers of prime values of these polynomials, and the numbers found agree very closely with the estimates for them provided by Li's recent modification of the Bateman–Horn Conjecture. While this does not prove that these polynomials take infinitely many prime values, it provides strong evidence for this, and it also adds extra support for the validity of the Bunyakovsky and Bateman–Horn Conjectures.

1. Introduction

The majority of applications of the famous Bateman–Horn Conjecture in Number Theory belong within that field. However, it may also be applied in other branches of Mathematics. In [24] we have shown how it can be applied within Group Theory. The aim of the present note is to show that it can also be useful in the combinatorial theories of block designs and of intersecting sets.

In [2], Amarra, Devillers and Praeger have recently constructed families of highly symmetric 2-designs which maximise certain parameters. Their construction depends on certain quadratic polynomials with integer coefficients taking prime power values. In [20] Hujdurović, Kutnar, Kuzma, Marušič, Miklavič and Orel have constructed permutation groups G of degree pq (p and q primes) with intersection densities $\rho(G) > 1$, as counterexamples to a conjecture by Meagher, Razafimahatratra and Spiga in [28]. Their construction, presented in an invited talk at G2S2 by Klavdija Kutnar, depends on certain cyclotomic polynomilals Φ_k taking prime values. In both cases these polynomials satisfy three simple necessary conditions which Bunyakovsky [7] in 1857 conjectured were also sufficient for any polynomial to take infinitely many prime values. Unfortunately, this conjecture has been proved only for polynomials of degree 1 (Dirichlet's Theorem on primes in an arithmetic progression). Nevertheless, the Bateman–Horn Conjecture [4], dating from 1962 and also proved only for degree 1, gives estimates $E(x)$ for the number $Q(x)$ of positive integers $t \le x$ at which a given polynomial takes prime values. Using a recent improvement to the Bateman–Horn

2010 *Mathematics Subject Classification.* 05B05, 11N32.

Key words and phrases. Block design, permutation group, intersection density, polynomial, prime number, Bateman–Horn Conjecture, Bunyakovsky Conjecture.

Conjecture due to Li [26], we calculated these estimates $E(x)$ for some of the simpler polynomials arising in [2], taking $x = 10^8$, and compared them with the actual numbers $Q(x)$ found by computer searches. As in various other applications of this conjecture (see [23, 24] for example), the estimates $E(x)$ are remarkably close to the actual values $Q(x)$. Although this does not prove the existence of infinite families of block designs or permutation groups in question, the accuracy of the estimates, together with the abundance of examples found, provides strong evidence for it, and it also adds to the growing body of evidence in favour of the more general Bunyakovsky and Bateman–Horn Conjectures.

There have been many number-theoretic applications of the Bateman–Horn Conjecture (see [1] for a survey), and a handful in areas such as combinatorics [15], cryptography [8, 32, 33, 34], elliptic curves [3, 13], error-correcting codes [25] and fast integer multiplication [12]. It seems likely that the present paper and [2] represent its first application to block designs, just as [23, 24] are the first in the areas of dessins d'enfants and permutation groups.

2. Primes versus prime powers

Although the problem in [2] requires prime power values of certain polynomials $f_{n,r}(t) \in \mathbb{Z}[t]$, it is easier to estimate the distribution of their prime values, using the Prime Number Theorem and conjectures based on it. This restriction is no great loss, as the vast majority of prime powers, up to any given large bound, are in fact prime: if $\pi(x)$ is the usual function counting primes $p \le x$, and $\Pi(x)$ is its analogue for prime powers $p^e \le x$, then $\pi(x)/\Pi(x) \to 1$ (quite rapidly) as $x \to \infty$. For example, $\pi(10^6)/\Pi(10^6) = 78\,498/78\,734 = 0.9970002\ldots$, while $\pi(10^9)/\Pi(10^9) = 50\,847\,534/50\,851\,223 = 0.999927\ldots$ (see [11]). Nevertheless, we carried out a more restricted search, over $t = 1, \ldots, 10^7$, for prime power values $f_{n,r}(t)$ of the chosen polynomials, finding just a few squares and one cube (see Section 12). However, in Section 14 we show how to realise any even power $p^{2i} > 9$ of an odd prime p as $f_{n,r}(0)$ for some polynomial $f_{n,r}$, a situation which has some interest for the construction of block designs.

3. The Bunyakovsky Conjecture

If a non-costant polynomial $f(t) \in \mathbb{Z}[t]$ is to take infinitely many prime values for $t \in \mathbb{N}$ (equivalently, if it is prime for infinitely many such t), then the following conditions must be satisfied:

(a) f must have a positive leading coefficient (otherwise it will take only finitely many positive values);
(b) f must be irreducible in $\mathbb{Z}[t]$ (otherwise all but finitely many of its values will be composite);
(c) f must not be identically zero modulo any prime p (otherwise all its values will be divisible by p).

In 1857 Bunyakovsky [7] conjectured that these three necessary conditions are also sufficient. (Condition (c) is needed to avoid examples such as $t^2 + t + 2$, which satisfies (a) and (b) but takes only even values.) For instance, if this were true it would imply Landau's conjecture (studied also by Euler [17]) that there are infinitely many primes of the form $t^2 + 1$. However, the Bunyakovsky Conjecture has been proved only in the case where f has degree 1: this is Dirichlet's Theorem,

that if a and b are coprime integers then there are infinitely many primes of the form $at + b$ (see [6, §5.3.2] for a proof).

4. The Bateman–Horn Conjecture

In 1962 Bateman and Horn [4] proposed a very general conjecture (in what follows we will use the abbreviation BHC) which comprises many previous conjectures and theorems and gives quantified versions of them. It deals with a finite set of polynomials simultaneously taking prime values. For our application to block designs it is sufficient to consider the case of a single polynomial, but in the case of permutation groups we need the full version of the BHC. If we incorporate a recent improvement due to Li [26], we get the following statement:

Conjecture 4.1 (Bateman and Horn, 1962; Li, 2019)**.** *Let $f_1, \dots, f_k \in \mathbb{Z}[t]$ be coprime polynomials satisfying conditions (a) and (b) of the Bunyakovsky Conjecture, and let their product $f = f_1 \cdots f_k$ satisfy condition (c). Denote by $Q(x)$ the number of $t \in \mathbb{N}$, $t \le x$, such that all $f_i(t)$, $i = 1, \dots, k$, are prime. Then the asymptotic estimate $E(x)$ for the number $Q(x)$ is given by the following formula:*

$$Q(x) \sim E(x) := C \int_a^x \frac{dt}{\prod_{i=1}^k \ln f_i(t)} \quad as \quad x \to \infty \tag{1}$$

where

$$C = C(f) := \prod_p \left(1 - \frac{1}{p}\right)^{-k} \left(1 - \frac{\omega_f(p)}{p}\right) \tag{2}$$

with the product over all primes p, and where $\omega_f(p)$ is the number of congruence classes $t \in \mathbb{Z}_p$ such that $f(t) = 0$. In (1), one chooses $a \ge 2$ large enough that the range of integration avoids singularities, where some $f_i(t) = 1$. (In our applications we can always take $a = 2$.)

Lemma 4.2 (Constant $C(f)$)**.** *The product in (2) converges to a constant $C > 0$.*

This statement is far from trivial. Bateman and Horn, in their original paper [4], limit themselves to a few hints. The first detailed proof was recently published in [1, Theorem 5.4.3], and it takes seven pages.

Since the integral in (1) diverges, we get the following

Corollary 4.3 (Infinitely many prime values)**.** *The estimate $E(x) \to \infty$ as $x \to \infty$; therefore, $Q(x)$ also goes to infinity: there are infinitely many integers $t \in \mathbb{N}$ such that all $f_i(t)$, $i = 1, \dots, k$, are simultaneously prime.*

As in the case of the Bunyakovsky Conjecture, the BHC, even when restricted to a single polynomial f, has been proved only in the case where $\deg f = 1$. This is the quantified version of Dirichlet's Theorem, that for fixed coprime a and b the number of $t \le x$ such that $at + b$ is prime is asymptotic to

$$\frac{1}{\varphi(a)} \int_2^x \frac{dt}{\ln(at + b)},$$

where φ is Euler's totient function. (Equivalently, the primes in the arithmetic progression $at + b$ are asymptotically equally distributed among the $\varphi(a)$ congruence classes of units mod a; see [6, §5.3.2] for a proof.)

An earlier special case of the BHC, applicable to a single quadratic polynomial f, is the Conjecture F of Hardy and Littlewood [19], giving similar estimates. For this reason, the constants $C(f)$ are sometimes known as Hardy–Littlewood constants.

5. Heuristic argument for the ingredients of the Bateman–Horn Conjecture

Here we give a heuristic argument to explain certain ingredients of the formula (1) for the Bateman–Horn estimate $E(x)$.

The Prime Number Theorem provides two asymptotic estimates for the number $\pi(x)$ of primes $p \le x$ as $x \to \infty$, namely

$$\pi(x) \sim \frac{x}{\ln x} \qquad \text{and} \qquad \pi(x) \sim \mathrm{Li}(x) := \int_2^x \frac{dt}{\ln t}. \tag{3}$$

The first is easy to use, but not very accurate; the second, involving the *offset logarithmic integral function* $\mathrm{Li}(x)$, is harder to use but much more accurate. For example, the number of primes up to 10^{28} has been computed by David Baugh, see Entry A006880 of [30]: it is equal to

$$\pi(10^{28}) \;=\; 157\,589\,269\,275\,973\,410\,412\,739\,598.$$

Now, the estimate by Hadamard and de la Vallée Poussin gives

$$\frac{10^{28}}{28 \cdot \ln 10} \;=\; 155\,105\,172\,108\,304\,224\,161\,117\,471.042$$

with the relative error $-1.576\,\%$, while the offset logarithmic integral function gives

$$\mathrm{Li}(10^{28}) \;=\; 157\,589\,269\,275\,974\,838\,158\,399\,970.696$$

with the relative error $0.000000000000906\,\% = 9.06 \cdot 10^{-13}\,\%$.

In either case, (3) suggests that one can regard $1/\ln x$ as the probability that x (or, rather, a randomly-chosen number close to x) is prime. Consider the "random variables" $\xi_i(t) = 1$ if $f_i(t)$ is prime, and $\xi_i(t) = 0$ otherwise. The "probability" that $\xi_i(t) = 1$ is $1/\ln f_i(t)$. If, in addition, we presume that these variables, for any given t, are independent, then the probability that all $f_i(t)$ are prime, or, in other words, the probability that the product $\eta(t) := \xi_1(t) \cdots \xi_k(t)$ is equal to 1, is $P(t) = \dfrac{1}{\prod_{i=1}^k \ln f_i(t)}$. Notice that the mean value of $\eta(t)$ is the expected value $\mathrm{E}(\eta(t)) = P(t)$.

The random variable $\eta(t)$ is a "counting function": as a first estimate for the number of $t \le x$ such that all $f_i(t)$ are prime, we may take the average number of times this variable is equal to 1. Let us choose a so that all $f_i(t) > 1$ for $t \ge a$. Then, as t goes from a to x, we have

$$\mathrm{E}\left(\sum_{t=a}^{x} \eta(t)\right) = \sum_{t=a}^{x} \mathrm{E}(\eta(t)) = \sum_{t=a}^{x} P(t) \approx \int_a^x P(t)dt = \int_a^x \frac{dt}{\prod_{i=1}^k \ln f_i(t)}. \tag{4}$$

We cannot present any profound reasons for considering $f_1(t), \ldots, f_k(t)$ as independent for any given t, but at least this assumption stands the test of a great number of experiments. However, the

same is not true when we vary the variable t. Therefore, a correcting term may be needed, and this is the constant $C(f)$.

First, if $f(t_0) \equiv 0 \bmod (p)$ for some integer t_0 and prime p, then $f(t) \equiv 0 \bmod (p)$ for all $t \equiv t_0 \bmod (p)$. We would like to avoid the situation when $f(t)$ is divisible by p (or, equivalently, at least one of $f_i(t)$ is divisible by p). The "probability" of the opposite event is $a_p = 1 - \frac{\omega_f(p)}{p}$.

Second, the probability that a "randomly chosen k-tuple of integers" (whatever that means) does not contain any element divisible by p is $b_p = \left(1 - \frac{1}{p}\right)^k$. The ratio a_p/b_p used in the product (2) resembles the conditional probability, though it is not one since it may well be > 1.

What remains is to assemble different parts of this Lego, but the corresponding procedure will need a long discussion and a self-coherent construction of a "probabilistic model" of what takes place, so we stop here. Anyway, we are not supposed to give a proof of the BHC; we only provide some plausible speculations on the matter. "The proof of the pudding is in the eating": the conjecture works well, even surprisingly well, and this is what is important about it.

6. The constant $C(f)$

Computing the constant $C(f)$ is a challenging problem in itself. As already mentioned above, the mere existence of a limit is a non-trivial fact. By the way, the convergence is not absolute: by changing the order of factors we may get a different limit value. This is not entirely surprising since the product $\prod_{p \le x}(1 - 1/p)^{-1}$ tends to infinity as $x \to \infty$ (according to Mertens [29], this product is asymptotically equivalent to $\ln(x)/\mu$ where $\mu = e^{-\gamma}$ and γ is the Euler–Mascheroni constant), while the product $\prod_{p \le x}(1 - \omega_f(p)/p)$ tends to zero. To make matters worse, the rate of convergence is, as one of our colleagues has put it, "frustratingly slow".

In Section 9 we discuss the computation of $\omega_f(p)$ for a single quadratic polynomial f. We will see that it involves rather subtle number-theoretic methods, mainly the quadratic reciprocity law. The case of cubic polynomials is treated in [35].

A highly advanced method, though still for a single polynomial, was proposed by H. Cohen [10]. For a quadratic polynomial it involves the techniques of L-functions and, in particular, of the Riemann ζ-function. For polynomials of degree greater than 2 one also needs to know the Galois group of the polynomial in question as well as the irreducible representations of this group. This subject is also treated in Sections 5.6 and 5.7 of the recently published book [5].

We have no intention to compete with the above specialists. Therefore, we have computed the products only over primes $p \le 10^8$. The constants $C(f)$ thus obtained already give excellent results in approximating the numbers of prime values of the polynomials we study in this paper.

Another interesting question is, how large (or how small) the constant C can be. Let us take, for example, the well-known Euler polynomial $f_1(t) = t^2 + t + 41$ (taking prime values for $t = 0, 1, 2, \ldots, 39$), and compare it with the polynomial $f_2(t) = t^2 + t + 75$. The constants $C(f_1)$ and $C(f_2)$ are computed in [10] with the precision of 39 digits[1]. They are:

$$C(f_1) = 6.6395463549428433306471137152997759329 38,$$
$$C(f_2) = 0.6219533598519743400087125748592568290 58.$$

[1]The values given in [10] must be multiplied by 2.

Since the integrals $\displaystyle\int_2^x \frac{dt}{\ln f_i(t)}$, $i = 1, 2$, are very close to each other for large x, we conclude that the first polynomial produces, approximately, 10.7 times as many primes as the second one.

Example 6.1 (Three pairs of polynomials)**.** It is instructive to compare the following three pairs of polynomials: $(f_1, f_2) = (t, t+2)$, $(g_1, g_2) = (t, 2t+1)$ and $(h_1, h_2) = (t, 3t-2)$. The first pair corresponds to twin primes, the second one to Sophie Germain primes, and the third one is encountered in the theory of divisible difference sets [18]. The equation $f(t) = t(t+2) \equiv 0 \bmod p$ has one root for $p = 2$ and two roots for all the other primes p. The corresponding constant is well known: $C(f) = 1.32032363169373914786\ldots$ The number of twin prime pairs is known up to 10^{18}: it is equal to 808 675 888 577 436, see Entry A007508 of [30]. Now, the BHC estimate gives

$$E(10^{18}) \;=\; C(f)\cdot\int_2^{10^{18}} \frac{dt}{\ln(t)\ln(t+2)} \;\approx\; C(f)\cdot\int_2^{10^{18}} \frac{dt}{\ln(t)^2} \;=\; 808\,675\,901\,493\,606.3$$

with the relative error 0.0000016 %.

It is easy to see that $C(g) = C(f)$ (indeed, the numbers $\omega_f(p)$ and $\omega_g(p)$ are always the same for every prime p), but the integral for the pair (g_1, g_2) is different: it is $\displaystyle\int_2^x \frac{dt}{\ln(t)\ln(2t+1)}$. Asymptotically, as $x \to \infty$, the two integrals are equivalent but the second one gives better estimates for the numbers of Sophie Germain primes (cf. Remark 11.1). For $t \le 10^{14}$ we have 132 822 315 652 pairs of Sophie Germain primes, see Entry A092816 of [30]. Now, computing the BHC estimate we get

$$E(10^{14}) \;=\; C(g)\cdot\int_2^{10^{14}} \frac{dt}{\ln(t)\ln(2t+1)} \;=\; 132\,822\,400\,531.22$$

with the relative error 0.000064 %. Note that, in spite of so accurate estimates, the infinitude of both the twin primes and the Sophie Germain primes remains unproved.

Finally, for the third pair, the number of solutions of the equation $h(t) = t(3t-2) = 0 \bmod p$ is the same as in the two previous examples, except for $p = 3$. Indeed, $\omega_f(3) = \omega_g(3) = 2$ while $\omega_h(3) = 1$. Therefore, the factor $1 - 2/3 = 1/3$ in $C(f)$ and $C(g)$ is replaced with $1 - 1/3 = 2/3$ in $C(h)$. Since the integrals are asymptotically equivalent, we conclude that the pair (h_1, h_2) produces, asymptotically, twice as many pairs of primes as the pairs (f_1, f_2) and (g_1, g_2), and the only reason for that is their different behaviour modulo $p = 3$.

A more systematic search for constants was carried out by Jacobson and Williams [21] (their paper contains many interesting examples) and by Rivin [31] (which is, mostly, an experimental work). Rivin carried out a large-scale experiment, computing thousands of constants $C(f)$ for randomly chosen polynomials. His observations do not yet have the status of conjectures, but they may be formulated as questions.

Questions 6.2 (Rivin [31])**.** Is it true that

(a) The mean value of $C(f)$ over a grand ensemble of polynomials f is 1?
(b) For monic polynomials f whose coefficients (other than the leading one) are bounded by N, the maximum value of $C(f)$ grows like $C_{\max} = O(\log\log N)$?

(c) The distribution of the values of $C(f)$ is log-normal?

7. Block designs

Here, in order to provide motivation for our particular choice of polynomials f, we briefly summarise the construction in [2] of block designs requiring certain polynomials to take prime power values.

A 2-(v, k, λ) *design* $\mathcal{D}$ consists of a set $\mathcal{P}$ of v points, together with a set $\mathcal{B}$ of k-element subsets of $\mathcal{P}$ called blocks, such that each pair of points lie in exactly λ blocks. (This implies that each point lies in the same number of blocks.) The *automorphisms* of $\mathcal{D}$ are the permutations of $\mathcal{P}$ which leave the set $\mathcal{B}$ invariant; they form a group $\mathrm{Aut}\,\mathcal{D}$.

If a subgroup $G \leq \mathrm{Aut}\,\mathcal{D}$ acts transitively on blocks then it also acts transitively on points. The latter action could be imprimitive, leaving invariant a partition C of $\mathcal{P}$ with $d \geq 2$ classes, each of size $c \geq 2$, so that $cd = v$. Delandtsheer and Doyen showed in [14] that in this case there exist positive integers m and n such that

$$mc + n = \binom{k}{2} = nd + m.$$

These integers m and n are the Delandtsheer-Doyen parameters of $\mathcal{D}$, with n and mc the numbers of unordered pairs of points in any given block, lying in the same or in different classes of C.

In [2], Amara, Devillers and Praeger have explored the restrictions these parameters place on subgroups G of $\mathrm{Aut}\,\mathcal{D}$. Let K denote the permutation group of degree d induced by G on the set of classes in C, and let H be the permutation group of degree c induced on any class in C by its setwise stabiliser in G, so that G is embedded in the wreath product $H \wr K \leq \mathrm{S}_c \wr \mathrm{S}_d$. The *rank* $\mathrm{Rank}(X)$ of any transitive permutation group X on a set Ω is the number of orbits of a point-stabiliser X_α ($\alpha \in \Omega$), or equivalently of X on $\Omega \times \Omega$; similarly, the *pair-rank* $\mathrm{PairRank}(X)$ is the number of orbits of X on unordered pairs of distinct elements of X, so that $(\mathrm{Rank}(X) - 1)/2 \leq \mathrm{PairRank}(X) \leq \mathrm{Rank}(X) - 1$. The main result of [2] is that in the above circumstances

$$\frac{\mathrm{Rank}(H) - 1}{2} \leq \mathrm{PairRank}(H) \leq n \quad \text{and} \quad \frac{\mathrm{Rank}(K) - 1}{2} \leq \mathrm{PairRank}(K) \leq m.$$

The authors of [2] give several constructions of designs $\mathcal{D}$ in which the ranks and pair-ranks of H and K attain these upper bounds. One construction requires *useful pairs* of integers n, c:

Definition 7.1 (Useful pair)**.** A pair of integers (n, c) is called *useful* (for this particular construction) if $n \geq 2$ and c is a prime power such that

$$c \equiv 1 \bmod (2n) \quad \text{and} \quad c + n = \binom{k}{2} \text{ for some integer } k \geq 2n.$$

They need c to be a prime power in order to define H to be the unique subgroup of index n in $\mathrm{AGL}_1(c)$, acting naturally on the field $\mathbb{F}_c$, while they take $K = \mathrm{S}_d$ acting naturally on $\mathbb{Z}_d$, so that $G := H \wr K$ has a transitive but imprimitive induced action on $\mathcal{P} = \mathbb{F}_c \times \mathbb{Z}_d$ with d classes of size c. By taking $d = 1 + \frac{c-1}{n}$ (the number of orbits of H on $\mathbb{F}_c$) and defining $\mathcal{B}$ to be the set of images under G of a carefully-chosen k-element subset $B \subset \mathcal{P}$ they obtain a 2-(cd, k, λ) design $\mathcal{D}$ for some

λ, admitting G as a block-transitive and point-imprimitive group of automorphisms. This design has Delandtsheer–Doyen parameters $m = 1$ and n, with $\mathrm{Rank}(H) = \mathrm{PairRank}(H) + 1 = n + 1$ and $\mathrm{Rank}(K) = \mathrm{PairRank}(K) + 1 = 2$.

The conditions for the pair n, c to be useful imply that, if r denotes the least positive remainder of k mod $(4n)$, then $\binom{r}{2} \equiv \binom{k}{2} \equiv n + 1 \bmod (2n)$. Thus, for fixed positive integers $n \geq 2$ and $r < 4n$ with $\binom{r}{2} \equiv n + 1 \bmod (2n)$ they need integers $k = 4nt + r$ for some integer $t \geq 0$ such that

$$f_{n,r}(t) := \binom{k}{2} - n = 8n^2t^2 + 2n(2r-1)t + \left(\frac{r(r-1)}{2} - n\right)$$

is a prime power c. If the polynomial $f_{n,r}$ takes prime power values for infinitely many integers $t \geq 0$ then this construction yields an infinite family of block designs with the required parameters and symmetry properties.

Example 7.2 (Two polynomials $f_{n,r}$)**.** The smallest "useful pair" (n, c) is $(2, 13)$, with $r = k = 6$ and $d = 7$, so that the corresponding design $\mathcal{D}$ has $cd = 91$ points and $|G| = 78^7 \cdot 7!$ automorphisms. This example arises from the polynomial $f_{n,r}(t) = f_{2,6}(t) = 32t^2 + 44t + 13$ taking the value $c = 13$ at $t = 0$. Note that $f_{2,6}(1) = 89$ is prime, giving a design on $cd = 89 \cdot 45 = 4005$ points with $|G| = (89 \cdot 44)^{45} \cdot 45!$, whereas $f_{2,6}(2) = 697 = 17 \cdot 41$ is not a prime power and therefore does not correspond to a design in this family.

Another useful pair is $(n, c) = (2, 53)$, with $k = 11$, $r = 3$ and $d = 7$, giving a smaller polynomial $f_{2,3}(t) = 32t^2 + 20t + 1$. This has its first prime power value $f_{2,3}(1) = 53$, giving a design on $53 \cdot 27 = 1431$ points with $|G| = (53 \cdot 26)^7 \cdot 7!$.

Note that, although this construction of block designs applies to any integer $t \geq 0$ such that $f_{n,r}(t)$ is a prime power, the number-theoretic conjectures and estimates we use are stated in terms of integers $t \geq 1$. This is not a problem here, since we are not concerned with individual block designs but with the existence or otherwise of infinite families of them. In any case, the value $f_{n,r}(0) = \frac{r(r-1)}{2} - n$ is easily dealt with (see Section 14).

8. Verifying the Bunyakovsky conditions

The polynomials f of interest in [2], and hence the main focus of this note, are those of the form

$$f(t) = f_{n,r}(t) = 8n^2t^2 + 2n(2r-1)t + \left(\frac{r(r-1)}{2} - n\right) \tag{5}$$

for integers $n \geq 2$ and $r \geq 1$ with

$$r < 4n \quad \text{and} \quad \frac{r(r-1)}{2} \equiv n + 1 \bmod (2n). \tag{6}$$

Note that this last condition implies that $r \geq 3$.

Lemma 8.1. *If a polynomial $f = f_{n,r}$ of the form (5) satisfies (6), it also satisfies Bunyakovsky's conditions (a) and (c); it satisfies his condition (b) if and only if n is not a triangular number $a(a+1)/2$, $a \in \mathbb{N}$.*

Proof. Clearly f satisfies condition (a) since $n \geq 1$. As a quadratic polynomial, f is reducible over $\mathbb{Z}$ if and only if its discriminant Δ is a perfect square. Here

$$\Delta = 4n^2(2r-1)^2 - 32n^2\left(\frac{r(r-1)}{2} - n\right) = 4n^2(8n+1), \tag{7}$$

and this is a square if and only if $8n+1$ is. Simple algebra shows that the solutions $n \in \mathbb{N}$ of $8n+1 = l^2$ ($l \in \mathbb{Z}$) are the triangular numbers $n = 1, 3, 6, 10, \ldots$, those of the form $a(a+1)/2$ for some $a = (l-1)/2 \in \mathbb{N}$ (readers may enjoy finding a geometric 'proof without words' for this), so f will satisfy (b) if and only if n does not have this form.

We now check condition (c). If a prime p divides $2n$ then f reduces mod (p) to a constant polynomial; this takes the value 1 since $r(r-1)/2 \equiv n+1 \bmod (2n)$, so f is not identically zero mod (p). If p does not divide $2n$ then f reduces to a quadratic polynomial, with at most two roots, so again it cannot be identically zero. □

In order to apply the Bateman–Horn Conjecture to the polynomials $f_{n,r}$, we therefore restrict attention to those for which n is not a triangular number.

9. Calculating $\omega_f(p)$ for $f_{n,r}$

Recall that $\omega_f(p)$, which appears in the infinite product (2), is the number of roots of f mod (p) for each prime p. We saw in the proof of Lemma 8.1 that $\omega_f(p) = 0$ for any prime p dividing $2n$. Primes p dividing $8n+1$ (and thus not dividing $2n$) give $\Delta \equiv 0 \bmod (p)$ by (7), and hence $\omega_f(p) = 1$ by the quadratic formula. Similarly, all other primes p give $\omega_f(p) = 2$ or 0 as $8n+1$ is or is not a quadratic residue (non-zero square) mod (p).

In general, given any prime p and integer q, one can determine whether or not q is a quadratic residue mod (p) by using the Legendre symbol

$$\left(\frac{q}{p}\right) = \begin{cases} 0 & \text{if } q \equiv 0 \bmod (p); \\ 1 & \text{if } q \text{ is a quadratic residue mod } (p); \\ -1 & \text{otherwise.} \end{cases}$$

(See [22, Chapter 7] for quadratic residues and the Legendre symbol.) Clearly

$$\left(\frac{q}{p}\right) = \left(\frac{q'}{p}\right) \quad \text{if } q \equiv q' \bmod (p),$$

and since the quadratic residues form a subgroup of index 2 in the group of units mod (p) we have the multiplicative property, that

$$\left(\frac{qq'}{p}\right) = \left(\frac{q}{p}\right)\left(\frac{q'}{p}\right)$$

for all $q, q' \in \mathbb{Z}$. Using these rules one can reduce the calculation of the Legendre symbol to the cases where q is an odd prime. In such cases one can use the Law of Quadratic Reciprocity, that if p and q are distinct odd primes then

$$\left(\frac{q}{p}\right) = \left(\frac{p}{q}\right) \quad \text{if } p \text{ or } q \equiv 1 \bmod (4),$$

while

$$\left(\frac{q}{p}\right) = -\left(\frac{p}{q}\right) \quad \text{if } p \equiv q \equiv -1 \bmod (4).$$

We also have

$$\left(\frac{2}{p}\right) = 1 \text{ or } -1 \quad \text{as} \quad p \equiv \pm 1 \text{ or } \pm 3 \bmod (8),$$

and

$$\left(\frac{-1}{p}\right) = 1 \text{ or } -1 \quad \text{as} \quad p \equiv 1 \text{ or } -1 \bmod (4).$$

By iterating these rules one can reduce the values of p and q until they are small enough to be dealt with by inspection.

We have seen that if $f = f_{n,r}$ then $\omega_f(p) = 0$ for all primes p dividing $2n$. For primes p not dividing $2n$, by the definitions of the function ω_f and the Legendre symbol, the quadratic formula gives $\omega_f(p) = \left(\frac{\Delta}{p}\right) + 1$. We will use this in the following examples.

Example 9.1. The smallest value of n which is not a triangular number is $n = 2$, giving $8n+1 = 17$. Since $17 \equiv 1 \bmod (4)$ we have

$$\left(\frac{17}{p}\right) = \left(\frac{p}{17}\right)$$

for any odd prime p. By squaring integers one sees that the quadratic residues mod (17) are $\pm 1, \pm 2, \pm 4$ and ± 8 (in fact, under multiplication mod (17) they form a cyclic group of order 8, generated by 2). Thus, if $f = f_{2,r}$ for some r then $\omega_f(p) = 2$ for odd primes $p \equiv \pm 1, \pm 2, \pm 4$ or ± 8 mod (17), while $\omega_f(p) = 0$ for primes $p \equiv \pm 3, \pm 5, \pm 6$ or ± 7 mod (17). For the remaining primes p we have $\omega_f(2) = 0$ and $\omega_f(17) = 1$.

Example 9.2. The second smallest value of n which is not a triangular number is $n = 4$, giving $8n + 1 = 33$. In this case multiplicativity and quadratic reciprocity give

$$\left(\frac{33}{p}\right) = \left(\frac{3}{p}\right)\left(\frac{11}{p}\right) = \left(\frac{p}{3}\right)\left(\frac{p}{11}\right)$$

for all odd primes $p \neq 3, 11$, since $3 \equiv 11 \bmod (4)$ so that any minus signs cancel. Now the quadratic residues mod (3) and mod (11) are 1 and $1, 3, 4, 5, 9$ respectively. The primes p for which 33 is a quadratic residue mod (p) are those which are both residues or both non-residues mod (3) and mod (11), so solving the relevant pairs of simultaneous congruences gives the classes $\pm 1, \pm 2, \pm 4, \pm 8, \pm 16$ mod (33) (forming a cyclic group generated by 2). If $f = f_{4,r}$ for some r then for odd primes p in these classes we have $\omega_f(p) = 2$, whereas for $p \equiv \pm 5, \pm 7, \pm 10, \pm 13, \pm 14$ mod (33) we have $\omega_f(p) = 0$. For the remaining primes p we have $\omega_f(2) = 0$ and $\omega_f(3) = \omega_f(11) = 1$.

Notice that the classes $\pm 3, \pm 6, \pm 9, \pm 12, \pm 15$ and ± 11 are not present in the above two lists: they are not coprime with 33 and therefore cannot be residues of a prime $p > 11$ modulo 33.

Example 9.3. The next case $n = 5$ is similar to Example 9.1 since $8n + 1 = 41$ is prime. We find that $\omega_f(2) = \omega_f(5) = 0$ and $\omega_f(41) = 1$, while for other primes p we have $\omega_f(p) = 2$ or 0 as p is or is not a quadratic residue mod (41). These are $\pm1, \pm2, \pm4, \pm5, \pm8, \pm9, \pm10, \pm16, \pm18, \pm20$.

For other permitted values of n the process is similar: thus for $n = 7$, 8 and 9 we have $8n + 1 = 57 = 3\cdot19$, $65 = 5\cdot13$ and 73 which is prime. However, in some cases the process can be lengthier, depending on the factorisation of $8n + 1$. We give just one more typical example.

Example 9.4. If $n = 13$ then $8n + 1 = 105 = 3 \cdot 5 \cdot 7$. Since $3 \equiv 7 \equiv -1 \bmod (4)$ while $5 \equiv 1 \bmod (4)$ we have

$$\left(\frac{105}{p}\right) = \left(\frac{3}{p}\right)\left(\frac{5}{p}\right)\left(\frac{7}{p}\right) = \left(\frac{p}{3}\right)\left(\frac{p}{5}\right)\left(\frac{p}{7}\right)$$

for all primes $p \geq 11$, so for such p we have $\omega_f(p) = 0$ or 2 as p is a quadratic residue modulo an even or odd number of the primes $3, 5$ and 7. Since the quadratic residues modulo these primes are generated by $1, -1$ and 2 respectively, this is easily determined in terms of congruences mod (105). (For some primes p, short-cuts are possible: for instance $105 \equiv -1 \bmod (53)$, so $\left(\frac{105}{53}\right) = \left(\frac{-1}{53}\right) = 1$, and similarly $\left(\frac{105}{107}\right) = \left(\frac{-1}{107}\right)\left(\frac{2}{107}\right) = (-1)^2 = 1$.) For $p = 3$, 5 or 7 we have $\omega_f(p) = 1$, while $\omega_f(2) = \omega_f(13) = 0$.

Since the values of $\omega_f(p)$ depend only on a few simple congruences for p, it is straightforward to program Maple to determine the factors in the infinite product (2) and hence to evaluate C. Note also that this part of the process depends only on n, and not on r, so that polynomials $f_{n,r}$ with the same parameter n can be dealt with simultaneously.

10. Evaluating the estimates

Since the factors in (2) approach 1 quite slowly as $p \to \infty$, convergence of this infinite product is rather slow, and one needs to multiply many terms in order to obtain good approximations for C. In our computations we used all the primes $p \leq 10^8$.

Maple calculates the definite integral in (1) by numerical quadrature. We found that running times were less than a second. Bateman and Horn simplified this part of the process by replacing $\ln(f(t))$ with $\deg(f)\ln(t)$ in (1), thus ignoring the leading coefficient of f together with all non-leading terms. No doubt, working in the early 1960s without resources such as Maple, they found that this shortcut was essential, especially in cases involving more than one polynomial. Li's recent improvement [26], using $\ln(f(t))$, certainly leads to more accurate estimates. In fact, the non-leading terms have remarkably little effect on the value of the integral (so again, r is almost irrelevant), whereas most of the extra accuracy comes from including the leading coefficient. For instance, the estimates $E(10^8)$ for the polynomials $f_{2,3}(t) = 32t^2+20t+1$ and $f_{2,6}(t) = 32t^2+44t+13$, given in the next section, differ by only 0.29.

For each polynomial f we used Maple to find the actual number $Q(x)$ of prime values of $f(t)$ for $t \leq x = 10^8$. Since, for example, $f_{5,r}(10^8) \approx 2 \cdot 10^{18}$, this was the most time-consuming part of our computations, with running times of about two hours on a modest laptop. Maple uses the Rabin–Miller primality test, which is probabilistic rather than deterministic. If an integer is prime,

the test will always declare it to be prime. If an integer is composite, the test may incorrectly declare it to be prime, but the probability of this happening is so small that in forty years of use of the test, no such incident has ever been reported. In our case, we found so many prime values of the polynomials f which we considered that, even if we have been very unlucky and a few of them are actually composite, this will have a negligible effect on our evidence.

11. The estimates and their accuracy

11.1. **The case $n = 2$.** The smallest allowed value for the parameter n is 2, so condition (6) implies that $r = 3$ or 6. In either case, evaluating $\omega_f(p)$ as in Example 9.1, and taking the product in (2) over all primes $p \le 10^8$, we found that $C = 4.721240276\ldots$ Putting $r = 3$ gives

$$f(t) = f_{2,3}(t) = 32t^2 + 20t + 1.$$

Taking $x = 10^i$ for $i = 3, 4, \ldots, 8$ we found the estimates $E(x)$ for the values of $Q(x)$ shown in Table 1. The final column, showing the relative error, reveals the accuracy of these estimates.

x	$Q(x)$	$E(x)$	relative error
10^3	326	314.49	−3.53%
10^4	2421	2404.86	−0.67%
10^5	19 394	19 438.26	0.23%
10^6	162 877	163 182.75	0.19%
10^7	1 405 448	1 406 630.14	0.084%
10^8	12 357 532	12 362 961.06	0.044%

Table 1. Numbers $Q(x)$ and estimates $E(x)$ for $f_{2,3}$.

11.2. **The cases with $n \le 9$.** The process for the remaining polynomials $f_{n,r}$ with non-triangular numbers $n \le 9$ was similar, with $x = 10^8$ in all cases. Table 2 summarises the results.

Remark 11.1 (Leading coefficient)**.** The greater the leading coefficient of a polynomial, the more significant is Li's improvement in [26] as compared with the initial Bateman–Horn formula in [4]. For example, in the case of $f(t) = f_{9,5}(t) = 648t^2 + 162t + 1$, we have two corresponding estimates

$$E_{\mathrm{Li}} = C \cdot \int_2^{10^8} \frac{dt}{\ln(f(t))} \quad \text{and} \quad E_{\mathrm{BH}} = \frac{C}{2} \cdot \int_2^{10^8} \frac{dt}{\ln(t)}$$

for $x = 10^8$, with relative errors 0.0046% and 18.7% respectively.

This does not contradict the fact that the two estimates are asymptotically equivalent. Indeed, the relative error of E_{BH} steadily decreases to approximately 2% when the upper limit x of the integration approaches 10^{70}. (Of course, we did not count the true number $Q(x)$ of prime values of this polynomial: instead, we took $E_{\mathrm{Li}}(x)$ as if it were the true value of $Q(x)$.)

(n, r)	$f_{(n,r)}(t)$	$C(f)$	$Q(10^8)$	$E(10^8)$	relative error
$(2, 3)$	$32t^2 + 20t + 1$	4.72124	12 357 532	12 362 961.06	0.0439%
$(2, 6)$	$32t^2 + 44t + 13$		12 363 849	12 362 960.77	−0.0072%
$(4, 7)$	$128t^2 + 104t + 17$	3.20688	8 100 174	8 102 333.64	0.0267%
$(4, 10)$	$128t^2 + 152t + 41$		8 104 531	8 102 333.57	−0.0271%
$(5, 4)$	$200t^2 + 70t + 1$	5.62398	14 052 016	14 050 339.22	−0.012%
$(5, 9)$	$200t^2 + 170t + 31$		14 049 951	14 050 339.05	0.003%
$(5, 12)$	$200t^2 + 230t + 61$		14 057 558	14 050 338.95	−0.051%
$(5, 17)$	$200t^2 + 330t + 131$		14 049 868	14 050 338.79	0.003%
$(7, 9)$	$392t^2 + 238t + 29$	3.82010	9 381 546	9 385 428.26	0.0415%
$(7, 13)$	$392t^2 + 350t + 71$		9 387 937	9 385 428.21	−0.0267%
$(7, 16)$	$392t^2 + 434t + 113$		9 385 853	9 385 428.17	−0.0045%
$(7, 20)$	$392t^2 + 546t + 183$		9 387 135	9 385 428.11	−0.0182%
$(8, 15)$	$512t^2 + 464t + 97$	3.22754	7 879 429	7 877 750.61	−0.0213%
$(8, 18)$	$512t^2 + 560t + 145$		7 879 013	7 877 750.57	−0.0160%
$(9, 5)$	$648t^2 + 162t + 1$	5.41032	13 129 138	13 129 743.85	0.0046%
$(9, 8)$	$648t^2 + 270t + 19$		13 127 661	13 129 739.69	0.0158%
$(9, 17)$	$648t^2 + 594t + 127$		13 129 080	13 129 739.55	0.0050%
$(9, 20)$	$648t^2 + 702t + 181$		13 130 890	13 129 743.63	−0.0087%
$(9, 29)$	$648t^2 + 1026t + 397$		13 128 036	13 129 743.50	0.0130%
$(9, 32)$	$648t^2 + 1134t + 487$		13 128 979	13 129 743.46	0.0058%

TABLE 2. Complete list of irreducible polynomials $f_{n,r}$ defined in (5) and satisfying conditions (6), for $n \le 9$. The constants $C(f)$ are computed over primes $p \le 10^8$.

12. PRIME POWER VALUES

We restricted our estimates to prime values of the polynomials $f_{n,r}$, since the Bunyakovsky and Bateman–Horn Conjectures have nothing to say about composite values. However, since the constructions of block designs in [2] apply to values which are prime powers, not just primes, we extended our computer searches to proper prime power values of some of these polynomials, for $t \le x = 10^7$.

As predicted in Section 2, we found very few proper prime power values, in comparison with the abundance of prime values. The values we found for $n \le 9$ and $t \le 10^7$ are shown in Table 3. We observe that there is only one cube: all the other prime powers are squares. The polynomials $f_{n,r}$ for the following pairs (n, r) with non-triangular parameters $n \le 9$ gave no proper prime power values for $t \le 10^7$, so they have been omitted from the table:

$$(2,6),\ (4,7),\ (4,10),\ (5,9),\ (5,12),\ (5,17),\ (7,9),\ (7,13),\ (7,16),\ (7,20),$$

$$(8,15),\ (8,18),\ (9,8),\ (9,20),\ (9,32).$$

(n, r)	polynomial $f_{n,r}$	$t \le 10^7$	$f_{n,r}(t)$	power
$(2, 3)$	$32t^2 + 20t + 1$	2	169	13^2
		8	2 209	47^2
		78	196 249	443^2
		282	2 550 409	$1\,597^2$
		9 590	2 943 171 001	$54\,251^2$
		23 666	17 923 019 113	$2\,617^3$
		90 372	261 348 955 729	$511\,223^2$
		3 069 998	301 596 468 440 089	$17\,366\,533^2$
$(5, 4)$	$200t^2 + 70t + 1$	4	3 481	59^2
		2 044	835 730 281	$28\,909^2$
		4 816	4 639 108 321	$68\,111^2$
		163 608	5 353 526 985 361	$2\,313\,769^2$
$(9, 5)$	$648t^2 + 162t + 1$	3 220	6 719 244 841	$81\,971^2$
$(9, 17)$	$648t^2 + 594t + 127$	1	1 369	37^2
		49	1 585 081	$1\,259^2$
$(9, 29)$	$648t^2 + 1\,026t + 397$	2	5 041	71^2

TABLE 3. Proper prime power values for irreducible polynomials $f_{n,r}$ with $n \le 9$, $t \le 10^7$

13. PRIME POWER VALUES OF REDUCIBLE POLYNOMIALS

A reducible polynomial $f(t) = g(t)h(t) \in \mathbb{Z}[t]$ can take only finitely many prime values (with $g(t)$ or $h(t)$ equal to ± 1), but could it take infinitely many prime power values? One way it might do so is if $g = h$ and this polynomial takes infinitely many prime values: Dirichlet's Theorem shows that this can happen with $\deg g = 1$, and the Bunyakovsky Conjecture suggests that it can happen with $\deg g > 1$. More generally, if g is irreducible and takes infinitely many prime values p, then any power $f = g^e$ of g takes infinitely many prime power values p^e. But what happens if f has two or more distinct irreducible factors?

Theorem 13.1. *If f is a polynomial in $\mathbb{Z}[t]$ with at least two different irreducible factors, then $f(t)$ is a prime power for only finitely many $t \in \mathbb{Z}$.*

Proof. We first deal with a simple special case, and with $t \ge 0$. Suppose that $f = gh$ for distinct factors $g(t) = a_k t^k + \cdots$ and $h(t) = b_k t^k + \cdots$ in $\mathbb{Z}[t]$ of the same degree $k \ge 1$. If there is some $t \in \mathbb{N}$ with $f(t) = p^e$ for a prime p and integer $e \ge 1$ then $g(t) = \pm p^i$ and $h(t) = \pm p^j$ for some integers $i, j \ge 0$ with $i + j = e$. If $i \ge j$ then

$$\frac{g(t)}{h(t)} = p^{i-j} \in \mathbb{Z}.$$

However, for all sufficiently large $t \in \mathbb{R}$ we have

$$\frac{g(t)}{h(t)} = \frac{a_k t^k + \cdots}{b_k t^k + \cdots} \to \frac{a_k}{b_k} \quad \text{strictly monotonically as } \ t \to +\infty,$$

so if there are infinitely many such $t \in \mathbb{N}$ with $i \geq j$ we have a sequence of integers p^{i-j} converging strictly monotonically to a_k/b_k, which is impossible. A similar argument, with the factors g and h transposed, shows that there can be only finitely many such $t \in \mathbb{N}$ with $i < j$, so $f(t)$ is a prime power for only finitely many $t \in \mathbb{N}$.

We can now deal with the general case, where f is reducible and not a power of a single irreducible polynomial. This allows us to factorise f in $\mathbb{Z}[t]$ as $f = gh$ where g and h have different irreducible factors. If $\deg g \neq \deg h$ we can replace f with

$$f^* = g^* h^* \quad \text{where} \quad g^* = g^{\deg h} \quad \text{and} \quad h^* = h^{\deg g},$$

so that f^* takes prime power values at the same integers t as f does. Since g^* and h^* are distinct but have the same degree, we can apply the preceding argument to show that f^* takes prime power values at only finitely many $t \in \mathbb{N}$, and hence the same applies to f. Finally, we can extend this result to all $t \in \mathbb{Z}$ either directly as above, using the fact that $g(t)/h(t)$ has similar limiting behaviour when $t \to -\infty$, or by applying the above argument for $t > 0$ to $f(-t)$, which factorises in the same way as $f(t)$. □

In particular, let $f = f_{n,r}$ in a case where this polynomial is reducible, or equivalently n is a triangular number $a(a+1)/2$ and Δ is a non-zero square $4n^2(8n+1) = 4n^2(2a+1)^2$. Then f factorises in $\mathbb{Z}[t]$ as

$$f(t) = g(t)h(t) = \frac{1}{2}(4nt + r + a)(4nt + r - a - 1),$$

where the first or second displayed linear polynomial has both of its coefficients even as $r \equiv a \bmod (2)$ or not, so that it absorbs the factor $\frac{1}{2}$. In either case, the resulting linear factors g and h of f in $\mathbb{Z}[t]$ are distinct and irreducible, so Theorem 13.1 implies that $f(t)$ is a prime power for only finitely many $t \in \mathbb{Z}$.

Proposition 13.2. *If $f_{n,r}$ is reducible and $n > 1$ then $f_{n,r}(t)$ is not a prime power for any integer $t \geq 1$.*

Proof. Suppose that $f := f_{n,r}$ is reducible and $n > 1$, so $n = a(a+1)/2$ for some integer $a \geq 2$ by Lemma 8.1, and that $f(t) = p^e$ for some prime p and integers $e, t \geq 1$.

Case 1 If $r \equiv a \bmod (2)$ then $f = gh$ where

$$g(t) = 2nt + \frac{r+a}{2} \quad \text{and} \quad h(t) = 4nt + r - a - 1.$$

Since $t \geq 1$ we have $g(t), h(t) > 1$ so $g(t) = p^i$ and $h(t) = p^j$ for integers $i, j \geq 1$ with $i + j = e$. If $i < j$ then

$$\frac{h(t)}{g(t)} = p^{j-i} \geq p \geq 2,$$

giving $-a - 1 \geq a$, which is impossible since $a \geq 1$. Thus $i \geq j$, so $g(t) \geq h(t)$, leading to

$$t \leq \frac{3a - r + 2}{4n} \leq \frac{3a+1}{2a(a+1)} < 1$$

(since $r \geq 1$ and $a \geq 2$), against our hypothesis.

Case 2 If $r \not\equiv a \bmod (2)$ then $f = gh$ where

$$g(t) = 4nt + r + a \quad \text{and} \quad h(t) = 2nt + \frac{r-a-1}{2}.$$

As before we have $g(t) = p^i$ and $h(t) = p^j$ for integers $i, j \geq 1$. If $i \leq j$ then $g(t) \leq h(t)$, leading to

$$2nt \leq \frac{r-a-1}{2} - (r+a) < 0,$$

which is impossible. Thus $i > j$, so

$$\frac{g(t)}{h(t)} = p^{i-j} \geq p.$$

If $p^{i-j} = 2$ then $g(t) = 2h(t)$, giving $a = -a - 1$, which is impossible. Hence $p^{i-j} \geq 3$, so $g(t) \geq 3h(t)$, leading to

$$t \leq \frac{a-r+3}{4n} \leq \frac{a}{4n} = \frac{1}{2(a+1)} < 1,$$

again contradicting our hypothesis. □

Remark 13.3. Although Theorem 13.1 applies to all $t \in \mathbb{Z}$, Proposition 13.2 applies only to integers $t \geq 0$ and cannot be extended to the case $t < 0$. For example, the polynomial

$$f(t) = f_{3,5}(t) = 72t^2 + 54t + 7 = (12t + 7)(6t + 1),$$

satisfies $f(-1) = 5^2$, with $g(-1) = h(-1) = -5$. Of course, negative values of t are not relevant to the 2-designs considered in this paper.

The condition $n > 1$ is required in Proposition 13.2, since the polynomial

$$f(t) = f_{1,1}(t) = 8t^2 + 2t - 1 = (2t + 1)(4t - 1)$$

satisfies $f(1) = 3^2$. The block designs $\mathcal{D}$ considered here all satisfy this condition.

14. Values at $t = 0$

Proposition 13.2 leaves open the possibility, which is relevant to 2-designs, that

$$f(0) = f_{n,r}(0) = \frac{r(r-1)}{2} - n$$

could be a prime power. Prime values $f_{n,r}(0)$ seem to arise quite frequently when $f_{n,r}$ is irreducible: for example, of the twenty polynomials in Table 2, sixteen have prime values at $t = 0$, three have the value 1, and $f_{8,18}$ has the value 145. However, the situation is rather different for reducible polynomials $f_{n,r}$, those for which n is a triangular number $a(a+1)/2$.

Proposition 14.1. *Let $f_{n,r}$ be reducible, and satisfy (5) and (6). Then $f_{n,r}(0)$ is a prime power p^e, $e \geq 1$, if and only if p is odd and one of the following occurs:*

a) *$e = 2i$ is even, with $n = (p^e - 1)/8 > 1$, $a = (p^i - 1)/2$ and $r = (3p^i + 1)/2$, or*
b) *$p^e = 7$, with $n = 3$, $a = 2$ and $r = 5$ (as in* Remark 13.3*).*

Note that by (a) every even power $p^e > 9$ of an odd prime p can be realised as a value $f_{n,r}(0)$ of a reducible polynomial $f_{n,r}$.

Example 14.2. One can realise 5^2 as a value by taking $n = 3$, $a = 2$ and $r = 8$. This gives

$$f(t) = f_{3,8}(t) = 72t^2 + 90t + 25 = (6t + 5)(12t + 5)$$

with $f(0) = 5^2$. Similarly, one can realise 7^2 by taking $n = 6$, $a = 3$ and $r = 11$, so that

$$f(t) = f_{6,11}(t) = 288t^2 + 252t + 49 = (12t + 7)(24t + 7)$$

with $f(0) = 7^2$. Taking $n = (13^4 - 1)/8 = 3\,570$ and $r = (3 \cdot 13^2 + 1)/2 = 254$ we get

$$f(t) = f_{n,r}(t) = 101\,959\,200\,t^2 + 3\,619\,980\,t + 28\,561 = (7\,140t + 169)(14\,280t + 169)$$

with $f(0) = 28\,561 = 13^4$.

Proof of Proposition 14.1. If we put $t = 0$ in Case (1) of the proof of Proposition 13.2, where $r \equiv a \bmod (2)$, we have

$$\frac{r + a}{2} = p^i \quad \text{and} \quad r - a - 1 = p^j$$

for integers $i, j \geq 0$ with $i + j = e \geq 1$ and $i \geq j$. Solving these simultaneous equations gives

$$r = p^i + \frac{p^j + 1}{2} \quad \text{and} \quad a = p^i - \frac{p^j + 1}{2},$$

so that

$$n = \frac{a(a + 1)}{2} = \frac{1}{8}\left((2p^i - p^j)^2 - 1\right).$$

(Recall that $f_{n,r}$ is reducible if and only if $8n + 1$ is a perfect square.) Here we require p^j to be odd, so that $r \equiv a \bmod (2)$; however, we reject solutions with $p = 2$ and $j = 0$ since they give $c = 2^i$ and $r(r - 1)/2 \not\equiv n + 1 \bmod (2n)$, contradicting condition (6), so p must be an odd prime.

The condition that $r(r - 1)/2 \equiv n + 1 \bmod (2n)$ also excludes many solutions when p is odd. We have

$$\frac{r(r - 1)}{2} - n - 1 = p^{i+j} - 1 \quad \text{and} \quad 2n = \frac{((2p^i - p^j)^2 - 1}{4},$$

so if $i > j$ then

$$0 < \frac{r(r - 1)}{2} - n - 1 < 2n$$

and hence $r(r - 1)/2 \not\equiv n + 1 \bmod (2n)$. However, if we take $i = j$ then

$$r = \frac{3p^i + 1}{2}, \quad a = \frac{p^i - 1}{2} \quad \text{and} \quad n = \frac{p^{2i} - 1}{8},$$

so that $r < 4n$ provided $p^i > 3$, and

$$\frac{r(r - 1)}{2} - n - 1 = p^{2i} - 1 = 8n \equiv 0 \bmod (2n)$$

as required. Thus every even power $p^e = p^{2i} > 9$ of an odd prime p is the value of some reducible polynomial $f_{n,r}$ at $t = 0$, giving conclusion (a).

A similar argument applies in Case (2) of the proof of Proposition 13.2, where $r \not\equiv a \bmod (2)$. We now have

$$r + a = p^i \quad \text{and} \quad \frac{r - a - 1}{2} = p^j,$$

with $i > j$, so that

$$r = \frac{p^i + 1}{2} + p^j \quad \text{and} \quad a = \frac{p^i - 1}{2} - p^j,$$

giving

$$n = \frac{a(a+1)}{2} = \frac{1}{8}\left((p^i - 2p^j)^2 - 1\right).$$

In this case

$$\frac{r(r-1)}{2} - n - 1 = p^{i+j} - 1 \quad \text{and} \quad 2n = \frac{((p^i - 2p^j)^2 - 1}{4}.$$

We need

$$p^{i+j} - 1 = \frac{r(r-1)}{2} - n - 1 \geq 2n = \frac{p^{2i} - 1}{4} - p^{i+j} + p^{2j}$$

so that

$$2p^{i+j} \geq \frac{p^{2i} + 3}{4} + p^{2j} > \frac{p^{2i}}{4}$$

and hence $p^{i-j} \leq 8$. Since $i > j$ and $p \geq 3$ this implies that $i - j = 1$ and $p = 3, 5$ or 7. Thus only odd powers p^e of these three primes can arise in Case 2.

Putting $i = j + 1$ gives

$$\frac{r(r-1)}{2} - n - 1 = p^{2j+1} - 1 \quad \text{and} \quad 2n = \frac{(p^{j+1} - 2p^j)^2 - 1}{4} = \frac{(p-2)^2 p^{2j} - 1}{4}.$$

Now $2n$ divides $\frac{r(r-1)}{2} - n - 1$, so multiplying by 4 shows that

$$8n = (p-2)^2 p^{2j} - 1 \quad \text{divides} \quad 4\left(\frac{r(r-1)}{2} - n - 1\right) = 4(p^{2j+1} - 1)$$

Defining $q := p^{2j}$, we see that $(p-2)^2 q - 1$ divides $4(pq - 1)$. We now apply this with $p = 3$, 5 and 7 in turn.

If $p = 3$ then $q - 1$ divides $12q - 4 = 12(q-1) + 8$, so $q - 1$ divides 8, giving $q = 1$ or 9. If $q = 1$ then $j = 0$, giving $r = 3$, $a = 0$ and $n = 0$, whereas we need $n > 1$. If $q = 9$ then $j = 1$, giving $r = 8$, $a = 1$ and $n = 1$, again too small. Thus $p \neq 3$.

If $p = 5$ then $9q - 1$ divides $20q - 4 = 2(9q - 1) + 2(q - 1)$ and hence $9q - 1$ divides $2(q - 1)$ giving $q = 1$. Then $j = 0$, so $r = 4$, $a = 1$ and $n = 1$, whereas we need $n > 1$. Thus $p \neq 5$.

If $p = 7$ then $25q - 1$ divides $28q - 4 = 25q - 1 + 3(q - 1)$ and hence $25q - 1$ divides $3(q - 1)$ giving $q = 1$. Then $j = 0$, so $r = 5$, $a = 2$ and $n = 3$, with $r < 4n$ and $r(r-1)/2 - n - 1 = 6 \equiv 0 \mod (2n)$; this gives the polynomial

$$f(t) = f_{3,5}(t) = 72t^2 + 54t + 7 = (12t + 7)(6t + 1)$$

in conclusion (b), with $f(0) = 7$. □

15. Intersection density of permutation groups

We now consider our second application. Permutations g and h of a set V are said to *intersect* if $g(v) = h(v)$ for some $v \in V$. The motivation for this is that if we define the *graph* of g to be the subset $\{(v, g(v)) \mid v \in V\}$ of V^2, then g and h intersect if and only if their graphs intersect. Thus intersecting families of permutations are special cases of intersecting families of sets.

Let G be a transitive permutation group of degree n, acting on a set V. A subset $\mathcal{F} \subseteq G$ is an *intersecting set* if each pair of elements of $\mathcal{F}$ intersect. For example, each coset gG_v ($v \in V$) of a point-stabiliser G_v is an intersecting set.

The *intersection density* of $\mathcal{F}$ is

$$\rho(\mathcal{F}) = \frac{|\mathcal{F}|}{|G_v|},$$

and the *intersection density* of G is

$$\rho(G) = \max_{\mathcal{F}} \rho(\mathcal{F}),$$

where $\mathcal{F}$ ranges over all intersecting sets in G. By taking $\mathcal{F} = G_v$ we see that $\rho(G) \geq 1$. By analogy with the Erdős–Ko–Rado Theorem [16], which gives an upper bound $\binom{n-1}{k-1}$ for the number of intersecting k-element subsets in an n-element set, we say that G has the *(strict) Erdős–Ko–Rado (or EKR) property* if $\rho(G) = 1$ (and if this upper bound is attained only by cosets of point-stabilisers). Thus $\rho(G)$ measures the extent to which G fails to have the EKR property.

In [28], Meagher et al. define

$$I(n) := \max_{G}\{\rho(G)\},$$

where G ranges over all transitive permutation groups of degree n. Their Conjecture 6.6 proposes a value for $I(n)$ for various integers n, including all those with at most two distinct prime factors. Some cases of that conjecture have already been proved. In case (iii) it is conjectured that $I(n) = 1$ if $n = pq$ for odd primes $p > q$. Hujdurović et al. in [20] prove this if G is imprimitive with q blocks of size p, but they construct counterexamples where G has p blocks of size q. These are constructed as follows from *projective primes*, which are defined in [24] as primes equal to the natural degree $(q^k - 1)/(q - 1)$ of $\mathrm{PSL}_k(q)$ for some prime power q.

Given a projective prime $p = (q^k - 1)/(q - 1)$ where q is an odd prime, let $n = pq$, define $V = \mathbb{Z}_q \times \mathbb{Z}_p$, and define a permutation

$$\alpha : (i, j) \mapsto (i, j + 1) \quad (i \in \mathbb{Z}_q, j \in \mathbb{Z}_p)$$

of V, a generator of G of order p. For the remaining generators, one needs a cyclic code C of length p and dimension k over the field $\mathbb{F}_q$, that is, a k-dimensional linear subspace of the p-dimensional vector space $\mathbb{F}_q^p$ which is invariant under the cyclic permutation $j \mapsto j + 1 \bmod (p)$ of the coordinates. The permutations

$$\beta_{\mathbf{c}} : (i, j) \mapsto (i + c_j, j)$$

of V for each $\mathbf{c} = (c_0, \ldots, c_{p-1}) \in C$ form a group K isomorphic to the additive group of C, with p orbits $\{(i, j) \mid i \in \mathbb{Z}_q\}$ for $j \in \mathbb{Z}_p$. The group G generated by α and K, a semidirect product $K \rtimes \langle\alpha\rangle$, is transitive but imprimitive on V, with the orbits of K forming p blocks of size q.

The required code C is constructed as the ideal of the ring $\mathbb{F}_q[x]/(x^p-1)$ annihilated by some monic irreducible factor $h(x)$ of the cyclotomic polynomial $\Phi_p(x)$ over $\mathbb{F}_q$, so that $\dim C = \deg h = k$. A standard result in coding theory [27, Equation 2.10] shows that since

$$\frac{q^k-1}{q-1} = \frac{p}{\gcd(p,q-1)} \quad (\text{both} = p),$$

all codewords $\mathbf{c} \neq \mathbf{0}$ have the same Hamming weight (number of non-zero coordinates), which is less than p. Thus each $\mathbf{c} \in C$ has at least one coordinate $c_j = 0$, so every element of K has a fixed point $v \in V$, and hence K is an intersecting set. Since $|G : K| = p$ and $|G : G_v| = pq$ we have $\rho(K) = q$, so $I(n) \geq \rho(G) \geq q > 1$, giving the required counterexample to case (iii) of the conjecture in [28]. (In fact, it is shown in [20] that $I(n) = \rho(G) = q$ for such values of n.)

It remains to consider the number and distribution of such projective primes

$$p = \frac{q^k-1}{q-1} = q^{k-1} + q^{k-2} + \cdots + 1$$

where q is prime. (For convenience we will include the case $q = 2$, with $p = 2^k - 1$ a Mersenne prime, even though it is not relevant to the construction in [20].) One can do this by applying the BHC to the polynomials $f_1(t) = t$ and $f_2(t) = t^{k-1} + t^{k-2} + \cdots + 1$. An obvious necessary condition for the irreducibility of f_2 is that k should be prime; in this case f_2 is the cyclotomic polynomial Φ_k, and hence is indeed irreducible. The other Bunyakovsky conditions are obviously satisfied by f_1 and f_2 for each odd prime k, so if the BHC is correct then for each such k there are infinitely many primes q such that p is prime, giving infinitely many counterexamples G to Conjecture 6.6(iii). (As we have shown in [24], this would fill a gap in the classification of permutation groups of prime degree by showing that for each prime $k \geq 3$ the group $\mathrm{PSL}_k(q)$, in its natural representation of degree $(q^k-1)/(q-1)$, has prime degree for infinitely many prime powers q.)

In fact, the BHC gives an estimate

$$E(x) = C_k \int_2^x \frac{dt}{\ln t \cdot \ln f_2(t)}$$

for the number $Q(x)$ of such primes $q \leq x$, where $C_k = C(f)$. Now for each prime r the roots of $f = f_1 f_2 \bmod (r)$ are 0 and, if k divides $r-1$, the $k-1$ primitive kth roots of 1 in $\mathbb{Z}_r$, so $\omega_f(r) = k$ or 1 as $r \equiv 1 \bmod (k)$ or not. This enables C_k to be calculated for each odd prime k.

As an example, for $k = 3$ we found 1 974 010 projective primes with prime $q \leq 10^9$, compared with a BHC estimate of 1 973 907.86 (see [24] for details). The smallest permutation group G in the corresponding family of counterexamples in [20] has degree 39, with $q = 3$ and $p = 13$, although an even smaller counterexample of degree 33, which does not arise from this construction, is also described there.

16. Conclusions

In the case of block designs we have found large numbers of prime values for many of those polynomials $f_{n,r}$ appearing in [2], each giving rise to a block design with specified parameters and symmetry properties. In the case of permutation groups we have found a large number of projective

primes with $k = 3$, providing counterexamples in [20] to Conjecture 6.6(iii) of [28]. In all cases the numbers found agree closely with the estimates for them provided by Li's recent version of the Bateman–Horn Conjecture. While this does not prove the conjectures that these polynomials take infinitely many prime values, and thus give infinite families of block designs and permutation groups, it provides strong evidence for this. Moreover, the accuracy of these estimates suggests that the same applies to those other polynomials $f_{n,r}$ and odd primes k for which we did not obtain computational evidence. Finally, we suggest that these investigations also provide extra support for the validity of the Bunyakovsky and Bateman–Horn Conjectures.

17. Acknowledgements

We are grateful to Yuri Bilu, to Cheryl Praeger and to Weixiong Li for many useful comments, and to the organisers of G2S2 2021 (Sochi) for the opportunity of publishing this paper. Alexander Zvonkin was partially supported by the ANR project Combiné (ANR-19-CE48-0011).

References

[1] S. L. Aletheia-Zomlefer, L. Fukshansky and S. R. Garcia, The Bateman–Horn conjecture: heuristics, history, and applications, *Expo. Math.* 38 (2020), 430–479. Also available at `arXiv-math[NT]:1807.08899v4`.

[2] C. Amarra, A. Devillers and C. E. Praeger, Delandsheer–Doyen parameters for block-transitive point-imprimitive block designs, `arXiv-math[CO]:2009.00282`.

[3] W. D. Banks, F. Pappalardi and I. E. Shparlinski On group structures realized by elliptic curves over arbitrary finite fields, *Exp. Math.* 21 (2012), 11–25.

[4] P. T. Bateman and R. A. Horn, A heuristic asymptotic formula concerning the distribution of prime numbers, *Math. Comp.* 16 (1962), 220–228.

[5] K. Belabas, H. Cohen, *Numerical Algorithms for Number Theory Using Pari/GP*, AMS, Mathematical Surveys and Monographs, vol. 254, 2021. All the programs used in the book may be downloaded via a link given on the page `https://www.math.u-bordeaux.fr/~kbelabas/Numerical_Algorithms/`.

[6] Z. I. Borevich and I. R. Shafarevich, *Number Theory*, Academic Press, New York and London, 1966.

[7] V. Bouniakowsky, Sur les diviseurs numériques invariables des fonctions rationnelles entières, *Mém. Acad. Sci. St. Péteresbourg*, 6e série, vol. VI (1857), 305–329.[2] Available at: `https://books.google.fr/books?hl=fr&id=wXIhAQAAMAAJ&pg=PA305#v=onepage&q&f=false`.

[8] J. Boxall and D. Gruenewald, Heuristics on pairing-friendly abelian varieties, *LMS J. Comput. Math.* 18 (2015), 419–443.

[9] Bunyakovsky conjecture, Wikipedia, `https://en.wikipedia.org/wiki/Bunyakovsky_conjecture`. Conjecture de Bouniakovsky, Wikipédia, `https://fr.wikipedia.org/wiki/Conjecture_de_Bouniakovski`.

[10] H. Cohen, High-precision computation of Hardy–Littlewood constants, Available at `https://oeis.org/A221712/a221712.pdf`.

[11] J. D. Cook, Distribution of prime powers, John D. Cook's blog, `https://www.johndcook.com/blog/2018/09/03/counting-prime-powers`.

[12] S. Covanov and E. Thomé, Fast integer multiplication using generalized Fermat primes, *Math. Comp.* 8 (2019), 1449–1477.

[2] Numerous publications give the following wrong title for Bunyakovsky's paper: "Nouveaux théorèmes relatifs à la distinction des nombres premiers et à la décomposition des entiers en facteurs". According to the French Wikipedia (see [9]), an article with this title does indeed exist, but it was published in 1840 and not in 1857, and it does not discuss the conjecture in question. The reader may also consult the original paper reproduced in the Google archive.

[13] C. David and E. Smith, A Cohen–Lenstra phenomenon for elliptic curves, *J. London Math. Soc. (2)* 89 (2014), 24–44.
[14] A. Delandtsheer and J. Doyen, Most block-transitive t-designs are point-primitive, *Geom. Dedicata* 29 (1989), 307–310.
[15] D. Ellis, G. Kalai and B. Narayanan, On symmetric intersecting families, *European J. Combin.* 86 (2020), 103094.
[16] P. Erdős, C. Ko and R. Rado, Intersection theorems for systems of finite sets, *Q. J. Math.* 12 (1961), 313–320.
[17] L. Euler, letter to Goldbach, 28th October 1752 (letter CXLIX), available at `http://eulerarchive.maa.org/correspondence/letters/OO0877.pdf`. See also De numeris primis valde magnis, *Novi Commentarii academiae scientiarum Petropolitanae* 9, 99–153 (1760); reprinted in *Commentat. arith.* 1, 356–378, 1849, and in *Opera Omnia: Ser. 1, vol. 3*, 1–45.
[18] G. A. Fernández-Alcober, R. Kwashira and L. Martínez, Cyclotomy over products of finite fields and combinatorial applications, *Europ. J. Comb.* 31 (2010), 1520–1538.
[19] G. H. Hardy and J. E. Littlewood, Some problems of 'Partitio numerorum'; III: On the expression of a number as a sum of primes, *Acta Math.* 114 (1923), 215–273.
[20] A. Hujdurović, K. Kutnar, B. Kuzma, D. Marušič, Š. Miklavič and M. Orel, On intersection density of transitive groups of degree a product of two odd primes, arXiv.math:2107.09327[CO].
[21] M. J. Jacobson, Jr., and H. G. Williams, New quadratic polynomials with high densities of prime values, *Math. Comp.* 72 (2002), no. 241, 499–519.
[22] G. A. Jones and J. M. Jones, *Elementary Number Theory*, Springer, 1998.
[23] G. A. Jones and A. K. Zvonkin, Klein's ten planar dessins of degree 11, and beyond, `https://arxiv.org/pdf/2104.12015.pdf`. To appear.
[24] G. A. Jones and A. K. Zvonkin, Groups of prime degree and the Bateman–Horn Conjecture, `https://arxiv.org/pdf/2106.00346.pdf`.
[25] D. Kim, Nonexistence of perfect 2-error-correcting Lee codes in certain dimensions, *European J. Combin.* 63 (2017), 1–5.
[26] W. Li, A note on the Bateman–Horn conjecture, *J. Number Theory* 208 (2020), 390–399. Also available at `https://arxiv.org/pdf/1906.03370.pdf`.
[27] R. J. McEliece, Irreducible cyclic codes and Gauss sums, in *Combinatorics (Proc. NATO Advanced Study Inst., Breukelen, 1974), Part I: Theory of designs, finite geometry and coding theory*, pp. 179–196, Math. Centre Tracts 55, Math. Centrum, Amsterdam, 1974.
[28] K. Meagher, A. S. Razafimahatratra and P. Spiga, On triangles in derangement graphs, *J. Combin. Theory, Ser. A* 180 (2021), 105390. Also available at `https://arxiv.org/pdf/2009.01086.pdf`.
[29] F. Mertens, Ein Beitrag zur analytischen Zahlentheorie, *J. reine angew. Math.* 78 (1874), 46–62.
[30] The Online Encyclopedia of Integer Sequences, `https://oeis.org`.
[31] I. Rivin, Some experiments on Bateman–Horn, 2015, `https://arxiv.org/pdf/1508.07821`.
[32] T. Scholl, Isolated elliptic curves and the MOV attack, *J. Math. Cryptol.* 11 (2017), 131–146.
[33] T. Scholl, Super-isolated elliptic curves and abelian surfaces in cryptography, *Exp. Math.* 28 (2019), 385–397.
[34] M. Sha, Heuristics of the Cocks–Pinch method, *Adv. Math. Commun.* 8 (2014), 103–118.
[35] D. Shanks and M. Lal, Bateman's constant reconsidered and the distribution of cubic residues, *Math. Comp.* 26 (1972), no. 117, 265–285.

School of Mathematical Sciences, University of Southampton, Southampton SO17 1BJ, UK
E-mail address: `G.A.Jones@maths.soton.ac.uk`

LaBRI, Université de Bordeaux, 351 Cours de la Libération, F-33405 Talence Cedex, France
E-mail address: `zvonkin@labri.fr`