Weil's character sum estimate and the universality of Paley graphs

László Babai

Last updated April 15, 2023

Read these notes in conjunction with the "Paley graphs and Paley tournaments" handout. If you do not feel comfortable with the notion of finite fields, replace all occurrences of the prime power q by the prime number p. The field $\mathbb{F}_p$ is simply $\mathbb{Z}_p$, the ring of residue classes modulo p.

1 Finite fields

Definition 1.1. A **field** is a set $\mathbb{F}$ with two binary operations, called addition and multiplication, and two distinct constants (special elements) called 0 and 1 (so $0 \neq 1$), such that we can perform the four arithmetic operations on $\mathbb{F}$ under the usual rules. Specifically, the two operations are commutative and associative, distributivity holds (multiplication distributes over addition), $(\forall a \in \mathbb{F})(0 + a = 1 \cdot a = a)$, every element a has an addtitive inverse $-a$, and every nonzero element a has a multiplicative inverse a^{-1}. The set of non-zero elements of the field $\mathbb{F}$ is called the **multiplicative group** of $\mathbb{F}$ and is denoted $\mathbb{F}^\times$.

Examples: $\mathbb{C}$ (complex numbers), $\mathbb{R}$ (real numbers), $\mathbb{Q}$ (rational numbers), $\mathbb{F}_p$ (the modulo p residue classes under operations defined by representatives). A notable non-example is $\mathbb{Z}$. (Why is $\mathbb{Z}$ not a field?)

Terminology 1.2. The number of elements of a field is called the **order of the field**. It may be finite or infinite. For example, $\mathbb{F}_p$ has order p.

Exercise 1.3. The order of every field is at least 2.

Theorem 1.4 (Galois, 1930)**.** *If $\mathbb{F}$ is a field then the order of $\mathbb{F}$ is a prime power, i. e., a number of the form $q = p^e$ where p is a prime number and $e \geq 1$. Moreover, for every prime power q there exists a field of order q, denoted $\mathbb{F}_q$. This field is unique up to isomorphism.*

The field $\mathbb{F}_q$ is also denote $\mathrm{GF}(q)$ ("Galois field"). If p is a prime then the finite field $\mathbb{F}_p$ is the same as $\mathbb{Z}_p$, the ring of residue classes modulo p.

Exercise 1.5. Show that the ring $\mathbb{Z}_n$ of residue classes modulo n is a field if and only if n is a prime number.

So in particular, if q is a prime power but not a prime number then $\mathbb{Z}_q$ is not a field. The construction of the $\mathbb{F}_q$ for $q = p^e$ relies on the existence of an irreducible polynomial of degree e over $\mathbb{F}_p$.

Definition 1.6. We say that $a \in \mathbb{F}_q$ is a **square** if $(\exists x \in \mathbb{F}_q)(a = x^2)$, and non-square otherwise.

Exercise 1.7. Let q be an **odd** prime power. Then there are $(q-1)/2$ squares and $(q-1)/2$ non-squares in $\mathbb{F}_q^\times$.

Exercise 1.8. Let q be an odd prime power. Prove that in $\mathbb{F}_q$, the product of two non-squares is a square.

Hint. Count: use the preceding exercise.

2 Order of elements, primitive roots

Definition 2.1. We say that the **order** of an element $a \in \mathbb{F}^\times$ is k if k is the smallest positive integer such that $a^k = 1$. If no such k exists, we say that the order of a is infinite. We write $o(a)$ for the order of a, except that we write $o(a) = 0$ if the order of a is infinite.

Exercise 2.2. Let $a \in \mathbb{F}^\times$ and let $n \in \mathbb{Z}$. Then $a^n = 1$ if and only if $o(a) \mid n$.

Note that this exercise is true even if the order of a is infinite, i. e., when $o(a) = 0$. In this case it says that $a^n = 1$ if and only if $n = 0$.

Definition 2.3. Let $z \in \mathbb{F}^\times$. For $n \geq 1$ we say that z is an **n-th root of unity** in $\mathbb{F}$ if $z^n = 1$, i. e., if $o(z) \mid n$.

Definition 2.4. For $n \geq 1$, we say that $z \in \mathbb{F}^\times$ is a **primitive n-th root of unity** if $o(z) = n$.

The following exercise generalizes Fermat's little Theorem to all finite fields.

Exercise 2.5. Let $a \in \mathbb{F}_q^\times$. Then $a^{q-1} = 1$.

In other words, the order of every element of $\mathbb{F}_q^\times$ is a divisor of $q - 1$.

Definition 2.6. A **primitive root** of the field $\mathbb{F}_q$ is an element of order $q - 1$.

Theorem 2.7 (Primitive roots)**.** *Every finite field has a primitive root.*

Exercise 2.8. If g is a primitive root of $\mathbb{F}_q$ then every element of $\mathbb{F}_q^\times$ is a power of g. If $a = g^\ell$ then ℓ is called the **discrete logarithm** of a to the base g. The discrete logarithm is unique modulo $q - 1$.

Exercise 2.9. Let q be an odd prime power. Let $a \in \mathbb{F}_q$. Then a is a square in $\mathbb{F}_q$ (i. e., $(\exists x \in \mathbb{F}_q)(a = x^2)$) if and only if $a^{(q-1)/2} = -1$.

Exercise 2.10. Let q be an odd prime power. The element $-1 \in \mathbb{F}_q$ is a square if and only if $q \equiv 1 \pmod 4$.

Definition 2.11. Let $\mathbb{N} = \{1, 2, \dots\}$ denote the set of natural numbers. The **Euler φ function** $\varphi : \mathbb{N} \to \mathbb{N}$ is defined as follows: $\varphi(n)$ is the number of integers in the interval $\{1, \dots, n\}$ that are relatively prime to n.

Exercise 2.12. (a) $\varphi(1) = \varphi(2) = 1$. (b) If p is a prime number then $\varphi(p) = p - 1$. (c) For a prime number p and $e \geq 0$ we have $\varphi(p^e) = p^e(1 - 1/p)$. (d) If $\gcd(a, b) = 1$ then $\varphi(ab) = \varphi(a) \cdot \varphi(b)$. (e) Let $n = p_1^{e_1} \cdots p_k^{e_k}$ be the prime-power decomposion of the positive integer n. Then

$$\varphi(n) = n \cdot \prod_{i=1}^{k} \left(1 - \frac{1}{p_i}\right). \tag{1}$$

Exercise 2.13. (a) The number of primitive roots in $\mathbb{F}_q$ is $\varphi(q - 1)$. (b) Let $k \mid q - 1$, $k \geq 0$. Then the number of elements of order k in $\mathbb{F}_q$ is $\varphi(k)$. (c) The number of primitive roots of order k in $\mathbb{C}$ is $\varphi(k)$.

3 Multiplicative characters

Let q be a prime power and $\mathbb{F}_q$ the corresponding finite field.

Definition 3.1. A **multiplicative character** of $\mathbb{F}_q$ is a function $\chi : \mathbb{F}_q \to \mathbb{C}$ such that $\chi(0) = 0$, $\chi(1) = 1$, and $(\forall a, b \in \mathbb{F}_q)(\chi(ab) = \chi(a)\chi(b))$.

Note that in the equation $\chi(1) = 1$, the two occurrences of "1" have different meaning: the first occurrence refers to the identity element of the field $\mathbb{F}_q$, the second, the identity element of the field $\mathbb{C}$. The analogous comment applies to the equation $\chi(0) = 0$. The actual meaning of the symbols 0 and 1 should always be clear from the context.

Convention 3.2. An **additive character** is a function $\psi : \mathbb{F}_q \to \mathbb{C}$ such that $(\forall a, b \in \mathbb{F}_q)(\psi(a + b) = \psi(a)\psi(b))$. In these notes we consider **multiplicative characters only**, so even if the adjective "multiplicative" is omitted, the term "character" will always refer to multiplicative characters.

Definition 3.3. The **principal character** χ_1 assigns the value 1 to each nonzero element of $\mathbb{F}_q$.

Definition 3.4. Let q be an odd prime power. The **quadratic character** χ_2 of $\mathbb{F}_q$ is defined by setting, for $a \in \mathbb{F}_q$,

$$\chi_2(a) = \begin{cases} 0 & \text{if } a = 0 \\ 1 & \text{if } a \neq 0 \text{ and } a \text{ is a square in } \mathbb{F}_q \\ -1 & \text{if } a \text{ is not a square in } \mathbb{F}_q \end{cases}$$

Exercise 3.5. Prove that χ_2 is a multiplicative character. (The hard case is covered by Ex. 1.8.)

Exercise 3.6. If χ is a multiplicative character of $\mathbb{F}_q$ then $\chi^{q-1} = \chi_1$.
This means that $(\forall a \in \mathbb{F}_q)((\chi(a))^{q-1} = \chi_1(a))$. So the statement is equivalent to saying that for all $a \in \mathbb{F}_q^\times$, the complex number $\chi(a)$ is a $(q-1)$-st complex root of unity.

Definition 3.7. The **order** of the multiplicative character $\chi : \mathbb{F}_q \to \mathbb{C}$ is the smallest positive k such that $\chi^k = \chi_1$. We denote the order of χ by $o(\chi)$.

Exercise 3.8. (a) For every multiplicative character χ we have $o(\chi) \mid q-1$. (b) $o(\chi_1) = 1$ (c) $o(\chi_2) = 2$.

Exercise 3.9. (a) χ_1 is the only multiplicative character of order 1. (b) χ_2 is the only multiplicative character of order 2.

Exercise 3.10. Let g be a primitive root in $\mathbb{F}_q$. A multiplicative character χ is determined by the value $\chi(g)$.
What this means is that if χ and ξ are two multiplicative characters of $\mathbb{F}_q$ and $\chi(g) = \xi(g)$ then $\chi = \xi$.

Exercise 3.11. The number of characters of $\mathbb{F}_q$ is $q-1$.

Exercise 3.12. Let $k \mid q-1$. The number of characters of $\mathbb{F}_q$ of order k is $\varphi(k)$.

Exercise 3.13. Let $\chi \neq \chi_1$ be a non-prinicipal multiplicative character of $\mathbb{F}_q$. Then $\sum_{x \in \mathbb{F}_q} \chi(x) = 0$.

Hint. Take $a \in \mathbb{F}_q$ such that $\chi(a) \neq 1$. Notice that the $\mathbb{F}_q \to \mathbb{F}_q$ map $x \mapsto ax$ is bijective.

Exercise 3.14. Let q be an odd prime power. Then $\sum_{a \in \mathbb{F}_q} \chi_2(a)\chi_2(a-1) = -1$.

Hint. For $a \neq 0$ write $a-1$ as $a(1-1/a)$.

Exercise 3.15. (Orthogonality) Let χ and ξ be two distinct multiplicative characters of $\mathbb{F}_q$. Then $\sum_{a \in \mathbb{F}_q} \chi(a)\overline{\xi(a)} = 0$. (Here $\overline{z}$ means the complex conjugate of the number z.)

4 André Weil's character sum estimate

Exercise 4.1. Let q be an odd prime power. Then $|\sum_{a \in \mathbb{F}_q} \chi_2(-a^2+2a-1)| = q-1$.

Exercise 4.2. Let q be an odd prime power. Then $\sum_{a \in \mathbb{F}_q} \chi_2(a^2+1) = -1$.

In each of the preceding two exercises we were looking at the quadratic character evaluated at values of a polynomial: $-x^2+2x-1$ in the first case and x^2+1 in the second case. We observe no cancellation of terms in the first case, and virtually all terms cancel out in the second case. The reason is that in the first case the polynomial is a constant times a square; in the second case, it is not. Of course the first exercise is straightforward; the second takes effort.

A far-reaching generalization of the second case was proved by André Weil in 1948.

Theorem 4.3 (Weil's character sum estimate)**.** *Let q be a prime power. Let χ be a multiplicative character of $\mathbb{F}_q$ of order $k = o(\chi)$. Let g be a polynomial of degree $d \geq 1$ over $\mathbb{F}_q$. Assume g is not of the form $c \cdot h^k$ where $c \in \mathbb{F}_q$ and h is a polynomial over $\mathbb{F}_q$. Then*

$$\left| \sum_{a \in \mathbb{F}_q} \chi(g(a)) \right| \leq (d-1)\sqrt{q}\,.$$

Let us understand what is happening here. Think of q being large and d small–we evaluate the character of a low-degree polynomial. We are adding up q quantities, at least $q - d$ of which have unit absolute value. (Why?) So the sum could potentially be close to q. Instead, it is now not much greater than $\sqrt{q}$. This means tremendous cancellation is occurring–the amount of cancellation is comparable to the cancellation in a sum of random ± 1 values.

Exercise 4.4. Let $X = \sum_{i=1}^{n} Y_i$ where the Y_i are independent random variables taking the value ± 1 with equal probability. Then the standard deviation of X is $\sqrt{n}$.

This observation makes Weil's Theorem a powerful *derandomization tool:* it permits us, in some cases, to give explicit construction of objects of which the existence is easily proved by the probabilistic method. An example is the analysis of small subgraphs of the Paley graph which we describe below.

Let us take a look at the necessity of Weil's assumption on the polynomial.

Exercise 4.5. If in Weil's Theorem we change the assumption on g to $g = c \cdot h^k$ for some $c \in \mathbb{F}_q$ and some polynomial h then

$$q - (d/k) \leq \left| \sum_{a \in \mathbb{F}_q} \chi(g(a)) \right| \leq q\,.$$

5 Paley graphs over finite fields

In this section, q is a prime power and $q \equiv 1 \pmod 4$.

Definition 5.1. The **Paley graph of order** q, denoted $\mathrm{PGr}(q)$, is defined as follows. The vertices of $\mathrm{PGr}(q)$ are the elements of the field $\mathbb{F}_q$. Vertices i and j are adjacent if $j - i$ is a non-zero square in $\mathbb{F}_q$.

Exercise 5.2. Show that this definition is sound: it indeed defines a graph. You need to show that the adjacency relation is symmetric. Show where you use the assumption that $q \equiv 1 \pmod 4$.

Exercise 5.3. Show that $\mathrm{PGr}(q)$ is (a) vertex-transitive (all vertices are equivalent under automorphisms) (b) edge-transitive (all edges are equivalent under automorphisms) (c) arc-transitive (all ordered pairs of adjacent vertices are equivalent under automorphisms).

Exercise 5.4. Show that $\mathrm{PGr}(q)$ is self-complementary (isomorphic to its complement).

Exercise 5.5. Show that every vertex of $\mathrm{PGr}(q)$ has degree $(q-1)/2$.

Exercise 5.6. Show that $\mathrm{PGr}(q)$ has diameter 2.

Hint. Prove the following, much more general statement. Let G be a graph with n of vertices. Assume every vertex has degree $\geq (n-1)/2$. Then the graph has diameter ≤ 2.

Exercise 5.7. (a) Show that every pair of adjacent vertices of $\mathrm{PGr}(q)$ has the same number of common neighbors. (b) Show that this number is $(q-5)/4$. (c) Show that every pair of distinct, non-adjacent vertices has the same number of common neighbors. (d) Show that this number is $(q-1)/4$.

Exercise 5.8. (a) Show that the adjacency matrix A of $\mathrm{PGr}(q)$ satisfies an equation of the form $A^2 + bA + cI = dJ$. Determine the coefficients b, c, d. (I is the identity matrix, J is the all-ones matrix.) (b) Find the eigenvalues of A. (c) Find the multiplicity of each eigenvalue of A.

6 Paley tournaments

In this section, q is a prime power and $q \equiv -1 \pmod 4$.

Definition 6.1. The **Paley tournament of order** q, denoted $\mathrm{PTr}(q)$, is defined as follows. The vertices of $\mathrm{PTr}(q)$ are the elements of the field $\mathbb{F}_q$. (i, j) is an edge (we draw the arrow $i \to j$) if $j - i$ is a non-zero square in $\mathbb{F}_q$.

Exercise 6.2. Show that this definition is sound: it indeed defines a tournament. You need to show that this is an orientation of the complete graph, i. e., for every pair $\{a, b\}$ of distinct vertices, exactly one of (a, b) and (b, a) is an edge. Show where you use the assumption that $q \equiv -1 \pmod 4$.

Exercise 6.3. Show that $\mathrm{PTr}(q)$ is (a) vertex-transitive (b) edge-transitive (all edges are equivalent under automorphisms).

Exercise 6.4. Show that $\mathrm{PTr}(q)$ is self-converse (isomorphic to its converse, where every edge is reversed).

Exercise 6.5. Show that every vertex of $\mathrm{PTr}(q)$ has indegree $(q-1)/2$ and the same outdegree. Show that this follows from vertex-transitivity.

Exercise 6.6. Show that the directed diameter of $\mathrm{PTr}(q)$ is 2, i. e., if $a \neq b$ are vertices then b can be reached from a in at most two steps.

Exercise 6.7. (a) Show that every edge (a, b) in $\mathrm{PTr}(q)$, the number of two-step walks from a to b is the same. (b) Show that this number is $(q-3)/4$. (c) Show that every edge (a, b) in $\mathrm{PTr}(q)$, the number of two-step walks from b to a is the same. (d) Show that this number is $(q+1)/4$.

Definition 6.8. Let $G = ([n], E)$ be an oriented graph. This means that the adjacency relation is antisymmetric: if $(u, v) \in E$ then $(v, u) \notin E$. We define the **$\pm$-adjacency matrix** $A = (a_{ij})$ of G as follows:

$$a_{ij} = \begin{cases} 1 & \text{if } (i,j) \in E \\ -1 & \text{if } (j,i) \in E \\ 0 & \text{otherwise} \end{cases}$$

Note that this includes $a_{ii} = 0$. If G is a tournament then $a_{ij} = 0 \iff i = j$.

Exercise 6.9. Let G be an oriented graph and let A be its $\pm$-adjacency matrix.
(a) Observe that $A^T = -A$.
(b) Assume $(\forall i,j)(\deg^+(i) = \deg^-(j))$ (all indegrees and outdegrees are equal). Then the all-ones vector is an eigenvector of A. What is the corresponding eigenvalue?
(c) If G is vertex-transitive then the assumption in (b) holds.

Exercise 6.10. Let A be the $\pm$-adjacency matrix of the Paley tournament $\mathrm{PTr}(q)$.
(i) Prove that A^2 can be expressed as $A^2 = aI + bJ$. Determine the coefficients a and b.
(ii) Determine the eigenvalues of A^2 and their multiplicities.
(iii) Determine the eigenvalues of A and their multiplicities (over $\mathbb{C}$).

7 k-universal graphs

Definition 7.1. We say that the graph G is **k-universal** if every graph with k vertices is isomorphic to some induced subgraph of G.

Exercise 7.2. For every $k \geq 1$ there exists a k-universal graph with $\leq k \cdot 2^{\binom{k}{2}}$ vertices.

This is very easy to show. We shall see that see that there exist much smaller k-universal graphs. Here is a simple lower bound so we can get a sense of what we should be shooting for.

Exercise 7.3. If G is a k-universal graph with n vertices then $n \geq 2^{(k-1)/2}$.

So we cannot get better than simply exponential in k (a bound of the form C^k for some constant $C > 1$). Below we outline the idea of such a bound.

Definition 7.4. We say that the graph $G = (V, E)$ has the **k-extension property** if $|V| \geq k$ and for all pairs (A, B) of subsets of V such that $A \cap B = \emptyset$ and $|A \cup B| = k$, there exists a vertex $x \in V$ that is adjacent to all vertices in A and to none of the vertices in B.

Exercise 7.5. If G has the k-extension property then G is $(k+1)$-universal.

Theorem 7.6 (Erdős)**.** *Let G be a random graph with n vertices in the uniform Erdős–Rényi model (edge probability 1/2). If $n \geq k^2 \cdot 2^k$ then whp G has the k-extension property. Consequently, if k is sufficiently large and $n \geq k^2 \cdot 2^k$ then there exists a $(k+1)$-universal graph with n vertices.*

Notation 7.7. "whp" stands for "with high probability." Since we now have two parameters, n and k, this requires an explanation. This result holds whp as $n \to \infty$ while k is a variable subject to the condition that $n \geq k^2 \cdot 2^k$. In other words, the following holds.
For every $\epsilon > 0$ there exists n_ϵ such that if $n \geq n_\epsilon$ and $n \geq k^2 \cdot 2^k$ then G has the k-extension property with probability $\geq 1 - \epsilon$.

This theorem gives a non-constructive proof of the existence of k-universal graphs of simply exponential size. In the next section we give a constructive proof at the cost of some increase in the size of the universal graph obtained, and a huge increase in the mathematical difficulty of the proof.

Exercise 7.8. Prove Theorem 7.6.

8 Application of Weil's character sum estimate: universality of Paley graphs

In this section we demonstrate an explicit construction of k-universal graphs of simply exponential size. The result derandomizes Theorem 7.6, at the cost of squaring the size of the graph. The graphs we show to be k-universal are the Paley graphs for sufficiently large q. The tool we use is Weil's character sum estimate.
As in the non-constructive proof of Theorem 7.6, we establish univesality via the k-extension property (Def. 7.4).

Theorem 8.1. *Let q be a prime power, $q \equiv 1 \pmod 4$. Assume $q > k^2 \cdot 4^k$. Then the Paley graph $\mathrm{PGr}(q)$ has the k-extension property (and is therefore $(k+1)$-universal).*

In the proof we shall use the following identity.

Exercise 8.2. Let $x_1, \ldots, x_n \in \mathbb{C}$. Then

$$\prod_{i=1}^{n}(1 + x_i) = \sum_{I \subseteq [n]} \prod_{i \in I} x_i \,. \tag{2}$$

Note that the sum on the right-hand side has 2^n terms.

Exercise 8.3. Use Weil's Theorem to prove Theorem 8.1. Follow the steps below.

Sketch of proof. Let $A, B \subset \mathbb{F}_q$, where $A \cap B = \emptyset$ and $|A \cup B| = k$. Let us say that $x \in \mathbb{F}_q$ is *good* for the pair (A, B) if $x \notin A \cup B$ and in the Paley graph $\mathrm{PGr}(q)$, x is adjacent to each $a \in A$ and not adjacent to any of the $b \in B$. We say that x is *bad* if x is not good and $x \notin A \cup B$. We say that x is *prohibited* if $x \in A \cup B$.

Let N denote the number of good vertices. We need to show that $N > 0$. In fact, we show more.

Theorem 8.4. *Using the notation above (beginning of Sketch of proof), we have*

$$\left| N - \frac{q}{2^k} \right| < k\sqrt{q} \,. \tag{3}$$

Remark 8.5. There is nothing random here, this holds for all pairs (A, B). But there is a probabilistic interpretation to this inequality. First let us conclude from the inequality that $\left|N - \frac{q-k}{2^k}\right| < (k+1)\sqrt{q}$. Now if the graph we are considering were random in the uniform Erdős–Rényi model then the expected number of good points would be $(q-k)/2^k$, and the standard deviation of the number of good points would be $\sqrt{q-k} \approx \sqrt{q}$. So we are talking about a tail bound in terms of a small multiple of the standard deviation. Find out what the Bernstein (Chernoff) bound would give in this situation, taking into account that we would need to use the union bound to get a result that holds for all pairs (A, B).
This gives concrete meaning to the idea that we are *derandomizing* the probabilistic proof.

We classified the elements of $\mathbb{F}_q$ as good, bad, or prohibited with respect to the pair (A, B). We now translate this classification into algebra by considering the following function $f : \mathbb{F}_q \to \mathbb{C}$. For $x \in \mathbb{F}_q$ let

$$f(x) = \prod_{a \in A}(1 + \chi_2(x-a)) \cdot \prod_{b \in B}(1 - \chi_2(x-b)) \,. \tag{4}$$

Show:

- If x is good then $f(x) = 2^k$.
- If x is bad then $f(x) = 0$.
- If x is prohibited then either $f(x) = 0$ or $f(x) = 2^{k-1}$.

Now proceed as follows.

(a) For $I \subseteq A \cup B$ let

$$g_I(x) = \prod_{a \in I \cap A}(x-a) \cdot \prod_{a \in I \cap B}(x-b) \tag{5}$$

Show that

$$f(x) = \sum_{I \subseteq A \cup B} (-1)^{|I \cap B|} \chi_2(g_I(x)) \,. \tag{6}$$

(b) Consider the sum
$S = \sum_{x \in \mathbb{F}_q} f(x)$. Show that $2^k N \le S \le 2^k N + k \cdot 2^{k-1}$.

(c) Observe that $\quad S = \displaystyle\sum_{I \subseteq A \cup B} (-1)^{|I \cap B|} \sum_{x \in \mathbb{F}_q} \chi_2(g_I(x)) \,.$

(d) Notice that the term corresponding to $I = \emptyset$ is q. We show that for sufficiently large q, this is the dominant term, meaning $N \approx q/2^k$, in accordance with the probabilistic interpretation discussed in Remark 8.5. All other terms (where $I \neq \emptyset$) only contribute "noise." The hard job is to show that the noise does not overwhelm the main term, and this is what Weil's estimate will do for us.

Let us write $S = q + R$. So $q + R \ge 2^k N \ge q + R - k \cdot 2^{k-1}$ and therefore

$$|2^k N - q| \le |R| + k \cdot 2^{k-1} \,. \tag{7}$$

(e) Use Weil's Theorem to give an upper bound on $|R|$:

$$|R| < (k-1) \cdot 2^k \cdot \sqrt{q}\,. \tag{8}$$

Make sure to verify that Weil's condition on the polynomials involved is met.

(f) Combine the last two items to show that

$$\left|N \cdot 2^k - q\right| < k \cdot 2^k \cdot \sqrt{q}\,. \tag{9}$$

proving Theorem 8.4. (Check!)

(g) Infer from this that if $q > k^2 \cdot 4^k$ then $N > 0$.

(h) Conclude that this completes the proof of Theorem 8.1. (Check!)

9 Problems

Exercise 9.1. Let p be a prime number and $k \geq 2$. Prove: If $p > k^2 \cdot 4^k$ then there exist k consecutive quadratic non-residues in $[p-1] = \{1, 2, \ldots, p-1\}$. (Use Weil's character sum estimate.)

Definition 9.2. Let $k \geq 1$. Let T be a tournament with n vertices. We say that a player x (a vertex) dominates a set A of players if x beats all players in A, i. e., for every $a \in A$, the edge $x \to a$ is in T. We say that T is **k-paradoxical** if $n \geq k$ and every set of k players is dominated by some player.

Explanation of the term. In such a tournament, it is difficult to rank the players: no matter how we rank them, there will be a player not among the top k who beat every player among the top k players.

Definition 9.3. In a **random tournament**, we fix the set of vertices and we orient each edge independently either way with probability 1/2.

Exercise 9.4. Prove that the Paley tournament PTr(7) is 2-paradoxical. Make your proof very simple, with no case-distinctions, based on what we know about the automorphisms of this tournament. Elegance matters.

Exercise 9.5. Let $k \geq 1$. Prove: If $n > k^2 \cdot 2^k$ then whp the random tournament is k-paradoxical.

The meaning of "whp" in this context (we have two parameters) is explained in Notation 7.7.

Exercise 9.6. Let $k \geq 2$ and let q be a prime power, $q \equiv -1 \pmod 4$. Prove: If $q > k^2 \cdot 4^k$ then the Paley tournament is k-paradoxical.