Smith explained part III

Peter Koymans
Max Planck Institute for Mathematics

MAX-PLANCK-GESELLSCHAFT

Informal Seminar

05 November 2020

Today's aim

Let $P(a, b)$ be the probability that a random $a \times a$ matrix (with coefficients in $\mathbb{F}_2$) has kernel of dimension b.

Today's aim

Let $P(a, b)$ be the probability that a random $a \times a$ matrix (with coefficients in $\mathbb{F}_2$) has kernel of dimension b.

Theorem 1

We have for all $n \geq 0$

$$\lim_{X \to \infty} \frac{|\{K \text{ im. quadr.} : D_K < X, \mathrm{rk}_4 \mathrm{Cl}(K) = n\}|}{|\{K \text{ im. quadr.} : D_K < X\}|} = \lim_{r \to \infty} P(r, n).$$

Today's aim

Let $P(a,b)$ be the probability that a random $a \times a$ matrix (with coefficients in $\mathbb{F}_2$) has kernel of dimension b.

Theorem 1

We have for all $n \geq 0$

$$\lim_{X\to\infty} \frac{|\{K \text{ im. quadr.} : D_K < X, \mathrm{rk}_4\mathrm{Cl}(K) = n\}|}{|\{K \text{ im. quadr.} : D_K < X\}|} = \lim_{r\to\infty} P(r,n).$$

Furthermore, for all $n \geq m \geq 0$

$$\lim_{X\to\infty} \frac{|\{K \text{ im. quadr.} : D_K < X, \mathrm{rk}_4\mathrm{Cl}(K) = n, \mathrm{rk}_8\mathrm{Cl}(K) = m\}|}{|\{K \text{ im. quadr.} : D_K < X, \mathrm{rk}_4\mathrm{Cl}(K) = n\}|} = P(n,m).$$

Main algebraic theorem

Write Art_x for the second Artin pairing of $\text{Cl}(x) := \text{Cl}(\mathbb{Q}(\sqrt{x}))$.

Theorem 2

Let p_1, p_2, q_1, q_2 be distinct prime numbers and let $d < 0$ be a squarefree integer coprime to the p_i and q_j. Take $a, b \mid d$. Suppose that $b \in 2\text{Cl}(dp_iq_j)[4]$ for all i and j. In case we have $\chi_a \in 2\text{Cl}^\vee(dp_iq_j)[4]$

$$\sum_{i=1}^{2}\sum_{j=1}^{2} \text{Art}_{dp_iq_j}(b, \chi_a) = 0.$$

Main algebraic theorem

Write Art_x for the second Artin pairing of $\text{Cl}(x) := \text{Cl}(\mathbb{Q}(\sqrt{x}))$.

Theorem 2

Let p_1, p_2, q_1, q_2 be distinct prime numbers and let $d < 0$ be a squarefree integer coprime to the p_i and q_j. Take $a, b \mid d$. Suppose that $b \in 2\text{Cl}(dp_iq_j)[4]$ for all i and j. In case we have $\chi_a \in 2\text{Cl}^\vee(dp_iq_j)[4]$

$$\sum_{i=1}^{2} \sum_{j=1}^{2} \text{Art}_{dp_iq_j}(b, \chi_a) = 0.$$

Next suppose that $\chi_{p_ia} \in 2\text{Cl}^\vee(dp_iq_j)[4]$ for all i and j. Then

$$\sum_{i=1}^{2} \sum_{j=1}^{2} \text{Art}_{dp_iq_j}(b, \chi_{p_ia}) = \sum_{r \mid b} \text{Frob}_{K_{p_1p_2, q_1q_2}/\mathbb{Q}}(r).$$

Main algebraic theorem

Write Art_x for the second Artin pairing of $\mathrm{Cl}(x) := \mathrm{Cl}(\mathbb{Q}(\sqrt{x}))$.

Theorem 2

Let p_1, p_2, q_1, q_2 be distinct prime numbers and let $d < 0$ be a squarefree integer coprime to the p_i and q_j. Take $a, b \mid d$. Suppose that $b \in 2\mathrm{Cl}(dp_iq_j)[4]$ for all i and j. In case we have $\chi_a \in 2\mathrm{Cl}^\vee(dp_iq_j)[4]$

$$\sum_{i=1}^{2}\sum_{j=1}^{2} \mathrm{Art}_{dp_iq_j}(b, \chi_a) = 0.$$

Next suppose that $\chi_{p_ia} \in 2\mathrm{Cl}^\vee(dp_iq_j)[4]$ for all i and j. Then

$$\sum_{i=1}^{2}\sum_{j=1}^{2} \mathrm{Art}_{dp_iq_j}(b, \chi_{p_ia}) = \sum_{r \mid b} \mathrm{Frob}_{K_{p_1p_2,q_1q_2}/\mathbb{Q}}(r).$$

Here $K_{p_1p_2,q_1q_2}$ is an unramified quadratic extension of $\mathbb{Q}(\sqrt{p_1p_2}, \sqrt{q_1q_2})$ with Galois group D_4 over $\mathbb{Q}$ and

$$\mathrm{Frob}_{K_{p_1p_2,q_1q_2}/\mathbb{Q}}(r) \in \mathrm{Gal}(K_{p_1p_2,q_1q_2}/\mathbb{Q}(\sqrt{p_1p_2}, \sqrt{q_1q_2})) \cong \mathbb{F}_2.$$

Main analytic theorem

To simplify matters, we will ignore all issues with small primes.

Main analytic theorem

To simplify matters, we will ignore all issues with small primes.

A Legendre specification is a function $a : \{(i, j) : 1 \leq i < j \leq r\} \to \{\pm 1\}$. To a Legendre specification and a product space X, we define $X(a)$ to be the subset of $x = (x_1, \ldots, x_r) \in X(a)$ such that

$$\left(\frac{x_i}{x_j}\right) = a(i, j).$$

Main analytic theorem

To simplify matters, we will ignore all issues with small primes.

A Legendre specification is a function $a : \{(i,j) : 1 \leq i < j \leq r\} \to \{\pm 1\}$. To a Legendre specification and a product space X, we define $X(a)$ to be the subset of $x = (x_1, \dots, x_r) \in X(a)$ such that

$$\left(\frac{x_i}{x_j}\right) = a(i,j).$$

Assumption 1

Let $X = X_1 \times \cdots \times X_r$ be a nice product space. Then we have for all Legendre specifications a

$$|X(a)| \approx \frac{|X|}{2^{r(r-1)/2}}.$$

Remark: $x, x' \in X(a)$ have the same Rédei matrix.

Combinatorial results

Let Y_1, Y_2 be non-empty sets and put $Y = Y_1 \times Y_2$. Put

$$V := \{F : Y \to \mathbb{F}_2\}, \quad W := \{g : Y \times Y \to \mathbb{F}_2\}.$$

Combinatorial results

Let Y_1, Y_2 be non-empty sets and put $Y = Y_1 \times Y_2$. Put

$$V := \{F : Y \to \mathbb{F}_2\}, \quad W := \{g : Y \times Y \to \mathbb{F}_2\}.$$

Let $d : V \to W$ be the linear map given by

$$dF((p_1, q_1), (p_2, q_2)) = F(p_1, q_1) + F(p_1, q_2) + F(p_2, q_1) + F(p_2, q_2).$$

Define $\mathcal{A}(Y) := \mathrm{im}(d)$.

Combinatorial results

Let Y_1, Y_2 be non-empty sets and put $Y = Y_1 \times Y_2$. Put

$$V := \{F : Y \to \mathbb{F}_2\}, \quad W := \{g : Y \times Y \to \mathbb{F}_2\}.$$

Let $d : V \to W$ be the linear map given by

$$dF((p_1, q_1), (p_2, q_2)) = F(p_1, q_1) + F(p_1, q_2) + F(p_2, q_1) + F(p_2, q_2).$$

Define $\mathcal{A}(Y) := \mathrm{im}(d)$.

Theorem 3

We have

$$\dim_{\mathbb{F}_2} \mathcal{A}(Y) = (|Y_1| - 1) \cdot (|Y_2| - 1).$$

Main combinatorial theorem

Call $g \in \mathcal{A}(Y)$ ϵ-bad if there exists $F : Y \to \mathbb{F}_2$ with $dF = g$ and

$$\left| F^{-1}(0) - \frac{|Y|}{2} \right| > \epsilon |Y|. \tag{1}$$

Main combinatorial theorem

Call $g \in \mathcal{A}(Y)$ ϵ-bad if there exists $F : Y \to \mathbb{F}_2$ with $dF = g$ and

$$\left| F^{-1}(0) - \frac{|Y|}{2} \right| > \epsilon |Y|. \tag{1}$$

Theorem 4

Let $\epsilon > 0$ be given. Then we have

$$\frac{|\{g \in \mathcal{A}(Y) : g \text{ is } \epsilon\text{-bad}\}|}{|\mathcal{A}(Y)|} \leq 2^{1+|X| - \prod_{i=1}^{2}(|X_i|-1)} \cdot \exp(-2\epsilon^2 |X|).$$

Main combinatorial theorem

Call $g \in \mathcal{A}(Y)$ ϵ-bad if there exists $F : Y \to \mathbb{F}_2$ with $dF = g$ and

$$\left| F^{-1}(0) - \frac{|Y|}{2} \right| > \epsilon |Y|. \tag{1}$$

Theorem 4

Let $\epsilon > 0$ be given. Then we have

$$\frac{|\{g \in \mathcal{A}(Y) : g \text{ is } \epsilon\text{-bad}\}|}{|\mathcal{A}(Y)|} \leq 2^{1+|X|-\prod_{i=1}^{2}(|X_i|-1)} \cdot \exp(-2\epsilon^2|X|).$$

Proof.

Bounding the F satisfying equation (1) using Hoeffding's inequality yields

$$2^{1+|X|} \exp(-2\epsilon^2|X|).$$

Then multiply this bound with the size of the kernel of d. □

Proof of main theorem

Consider the squarefree integers up to a large parameter N. Let r be an integer satisfying

$$|r - \log\log N| < (\log\log N)^{2/3}. \tag{2}$$

Proof of main theorem

Consider the squarefree integers up to a large parameter N. Let r be an integer satisfying

$$|r - \log\log N| < (\log\log N)^{2/3}. \tag{2}$$

Reduction step I: we will prove that the theorem holds within the set of squarefree integers with r prime divisors with r satisfying (2).

Proof of main theorem

Consider the squarefree integers up to a large parameter N. Let r be an integer satisfying

$$|r - \log\log N| < (\log\log N)^{2/3}. \tag{2}$$

Reduction step I: we will prove that the theorem holds within the set of squarefree integers with r prime divisors with r satisfying (2).

Reduction step II: we will prove that the theorem holds within the set of nice boxes $X = X_1 \times \cdots \times X_r$ with r satisfying (2).

Bad Legendre matrices

We would next like to consider sets of the shape $X(a)$. We throw away the following Legendre specifications a

Bad Legendre matrices

We would next like to consider sets of the shape $X(a)$. We throw away the following Legendre specifications a

- in case the 4-rank of elements in $X(a)$ is exceedingly large;
- we want the left and right kernel of the Rédei matrix to be as "unrelated" as possible.

Bad Legendre matrices

We would next like to consider sets of the shape $X(a)$. We throw away the following Legendre specifications a

- in case the 4-rank of elements in $X(a)$ is exceedingly large;
- we want the left and right kernel of the Rédei matrix to be as "unrelated" as possible.

By our fundamental assumption that $|X(a)|$ is of the correct size, this becomes a combinatorial problem about matrices. From now on suppose that the 4-rank is 2 and we will make the second condition explicit.

Bad Legendre matrices

We would next like to consider sets of the shape $X(a)$. We throw away the following Legendre specifications a

- in case the 4-rank of elements in $X(a)$ is exceedingly large;
- we want the left and right kernel of the Rédei matrix to be as "unrelated" as possible.

By our fundamental assumption that $|X(a)|$ is of the correct size, this becomes a combinatorial problem about matrices. From now on suppose that the 4-rank is 2 and we will make the second condition explicit.

Take a basis $c_1, c_2 \in \mathbb{F}_2^r$ for the characters in $2\mathrm{Cl}^\vee(K)[4]$, and a basis $i_1, i_2 \in \mathbb{F}_2^r$ for the ideals in $2\mathrm{Cl}(K)[4]$. We want

$$|\{v \in \{1, \ldots, r\} : \pi_v(x_1 c_1 + x_2 c_2 + x_3 i_1 + x_4 i_2) = 1\}| \approx \frac{r}{2}$$

for every non-trivial $(x_1, x_2, x_3, x_4) \in \mathbb{F}_2^4$.

Reduction to characters

We want to show that every matrix Art_x occurs equally often as x ranges over $X(a)$.

Reduction to characters

We want to show that every matrix Art_x occurs equally often as x ranges over $X(a)$.

Take a non-trivial character ρ from 2×2-matrices to $\mathbb{F}_2$.

Reduction to characters

We want to show that every matrix Art_x occurs equally often as x ranges over $X(a)$.

Take a non-trivial character ρ from 2×2-matrices to $\mathbb{F}_2$.

Reduction step IV: we need to estimate the sum

$$\sum_{x \in X(a)} \rho(\mathrm{Art}_x)$$

for each non-trivial character ρ.

Reduction to characters

We want to show that every matrix Art_x occurs equally often as x ranges over $X(a)$.

Take a non-trivial character ρ from 2×2-matrices to $\mathbb{F}_2$.

Reduction step IV: we need to estimate the sum

$$\sum_{x \in X(a)} \rho(\mathrm{Art}_x)$$

for each non-trivial character ρ.

As an example let us take the following character ρ that sends a matrix to the sum in the top row. Then we get

$$\sum_{x \in X(a)} \mathrm{Art}_x(i_1, c_1) + \mathrm{Art}_x(i_1, c_2).$$

Variable indices

Pick a small index z_1 with $\pi_{z_1}(c_1) = 1$, $\pi_{z_1}(c_2) = \pi_{z_1}(i_1) = \pi_{z_1}(i_2) = 0$.
Also pick a small index z_2 with $\pi_{z_2}(c_1) = \pi_{z_2}(c_2) = \pi_{z_2}(i_1) = \pi_{z_2}(i_2) = 0$.
Finally pick a large index z_{Cheb} for which $\pi_{z_{\text{Cheb}}}(i_1) = 1$, but the other projections are 0.

Variable indices

Pick a small index z_1 with $\pi_{z_1}(c_1) = 1$, $\pi_{z_1}(c_2) = \pi_{z_1}(i_1) = \pi_{z_1}(i_2) = 0$. Also pick a small index z_2 with $\pi_{z_2}(c_1) = \pi_{z_2}(c_2) = \pi_{z_2}(i_1) = \pi_{z_2}(i_2) = 0$. Finally pick a large index z_{Cheb} for which $\pi_{z_{\mathrm{Cheb}}}(i_1) = 1$, but the other projections are 0.

Reduction step V: for every element

$$P \in \prod_{\substack{j=1 \\ j \neq z_1, z_2}}^{k_{\mathrm{gap}}} X_i$$

prove equidistribution of

$$\sum_{\substack{x \in X(a) \\ \pi_{[k_{\mathrm{gap}}] - \{z_1, z_2\}}(x) = P}} \mathrm{Art}_x(i_1, c_1) + \mathrm{Art}_x(i_1, c_2).$$

Variable indices II

Rreduction step VI (HARD): for every element

$$Q \in \prod_{\substack{j=1 \\ j \neq z_1, z_2, z_{\text{Cheb}}}}^{r} X_i$$

and for two small subsets $Y_{z_1} \subseteq X_{z_1}$ and $Y_{z_2} \subseteq X_{z_2}$ show that

$$\sum_{x \in Y_{z_1} \times Y_{z_2} \times X^{\dagger}_{z_{\text{Cheb}}} \times Q} \text{Art}_x(i_1, c_1) + \text{Art}_x(i_1, c_2)$$

with $Y_1 \times Y_2$ consistent with Q and a and $X^{\dagger}_{z_{\text{Cheb}}}$ the subset of $X_{z_{\text{Cheb}}}$ consistent with $Y_1 \times Y_2$, Q and a.

Finishing the proof: moral idea

We get the linear equations

$$\mathrm{Art}_{dp_iq_k}(i_1, c_1) + \mathrm{Art}_{dp_iq_l}(i_1, c_1) + \mathrm{Art}_{dp_jq_k}(i_1, c_1) + \mathrm{Art}_{dp_jq_l}(i_1, c_1) = RHS.$$

There are $|Y_{z_1} \times Y_{z_2}|$ variables on the LHS, while there are $(|Y_{z_1}| - 1)(|Y_{z_2}| - 1)$ independent equations.

Finishing the proof: moral idea

We get the linear equations

$$\mathrm{Art}_{dp_iq_k}(i_1, c_1) + \mathrm{Art}_{dp_iq_l}(i_1, c_1) + \mathrm{Art}_{dp_jq_k}(i_1, c_1) + \mathrm{Art}_{dp_jq_l}(i_1, c_1) = RHS.$$

There are $|Y_{z_1} \times Y_{z_2}|$ variables on the LHS, while there are $(|Y_{z_1}| - 1)(|Y_{z_2}| - 1)$ independent equations.

The RHS behaves randomly by Chebotarev.

Finishing the proof: moral idea

We get the linear equations

$$\mathrm{Art}_{dp_i q_k}(i_1, c_1) + \mathrm{Art}_{dp_i q_l}(i_1, c_1) + \mathrm{Art}_{dp_j q_k}(i_1, c_1) + \mathrm{Art}_{dp_j q_l}(i_1, c_1) = RHS.$$

There are $|Y_{z_1} \times Y_{z_2}|$ variables on the LHS, while there are $(|Y_{z_1}| - 1)(|Y_{z_2}| - 1)$ independent equations.

The RHS behaves randomly by Chebotarev.

More formally it is a random additive function in $\mathcal{A}(Y_{z_1} \times Y_{z_2})$.

Finishing the proof: moral idea

We get the linear equations

$$\mathrm{Art}_{dp_iq_k}(i_1, c_1) + \mathrm{Art}_{dp_iq_l}(i_1, c_1) + \mathrm{Art}_{dp_jq_k}(i_1, c_1) + \mathrm{Art}_{dp_jq_l}(i_1, c_1) = RHS.$$

There are $|Y_{z_1} \times Y_{z_2}|$ variables on the LHS, while there are $(|Y_{z_1}| - 1)(|Y_{z_2}| - 1)$ independent equations.

The RHS behaves randomly by Chebotarev.

More formally it is a random additive function in $\mathcal{A}(Y_{z_1} \times Y_{z_2})$.

The system is underdetermined, so we can not solve for Art. But fortunately the system is only barely underdetermined.

Finishing the proof: moral idea

We get the linear equations

$$\mathrm{Art}_{dp_iq_k}(i_1, c_1) + \mathrm{Art}_{dp_iq_l}(i_1, c_1) + \mathrm{Art}_{dp_jq_k}(i_1, c_1) + \mathrm{Art}_{dp_jq_l}(i_1, c_1) = RHS.$$

There are $|Y_{z_1} \times Y_{z_2}|$ variables on the LHS, while there are $(|Y_{z_1}| - 1)(|Y_{z_2}| - 1)$ independent equations.

The RHS behaves randomly by Chebotarev.

More formally it is a random additive function in $\mathcal{A}(Y_{z_1} \times Y_{z_2})$.

The system is underdetermined, so we can not solve for Art. But fortunately the system is only barely underdetermined.

Then it is still true that for almost all choices of RHS we have that all choices of Art satisfying the equations are equidistributed.

Finishing the proof

Now put

$$F = \mathrm{Art}_x(i_1, c_1) + \mathrm{Art}_x(i_1, c_2).$$

Finishing the proof

Now put

$$F = \mathrm{Art}_x(i_1, c_1) + \mathrm{Art}_x(i_1, c_2).$$

Define

$$M := \prod_{p_1, p_2 \in Y_{z_1}} \prod_{q_1, q_2 \in Y_{z_2}} K_{p_1 p_2, q_1 q_2}.$$

Finishing the proof

Now put

$$F = \mathrm{Art}_x(i_1, c_1) + \mathrm{Art}_x(i_1, c_2).$$

Define

$$M := \prod_{p_1, p_2 \in Y_{z_1}} \prod_{q_1, q_2 \in Y_{z_2}} K_{p_1 p_2, q_1 q_2}.$$

Then it follows from the main algebraic result

$$dF((p_1, q_1, x), (p_2, q_2, x)) = \mathrm{Frob}_{K_{p_1 p_2, q_1 q_2}/\mathbb{Q}}(\pi_{z_{\mathrm{Cheb}}}(x)) + g_0$$

with $g_0 \in \mathcal{A}(Y_{z_1} \times Y_{z_2})$ not depending on $\pi_{z_{\mathrm{Cheb}}}(x)$.

Finishing the proof

Now put

$$F = \mathrm{Art}_x(i_1, c_1) + \mathrm{Art}_x(i_1, c_2).$$

Define

$$M := \prod_{p_1, p_2 \in Y_{z_1}} \prod_{q_1, q_2 \in Y_{z_2}} K_{p_1 p_2, q_1 q_2}.$$

Then it follows from the main algebraic result

$$dF((p_1, q_1, x), (p_2, q_2, x)) = \mathrm{Frob}_{K_{p_1 p_2, q_1 q_2}/\mathbb{Q}}(\pi_{z_{\mathrm{Cheb}}}(x)) + g_0$$

with $g_0 \in \mathcal{A}(Y_{z_1} \times Y_{z_2})$ not depending on $\pi_{z_{\mathrm{Cheb}}}(x)$.

Now consider the map $X_{z_{\mathrm{Cheb}}} \to \mathrm{Gal}(M/\mathbb{Q})$ that sends

$$r \mapsto \mathrm{Frob}_{M/\mathbb{Q}}(r).$$

Finishing the proof

Now put

$$F = \text{Art}_x(i_1, c_1) + \text{Art}_x(i_1, c_2).$$

Define

$$M := \prod_{p_1, p_2 \in Y_{z_1}} \prod_{q_1, q_2 \in Y_{z_2}} K_{p_1 p_2, q_1 q_2}.$$

Then it follows from the main algebraic result

$$dF((p_1, q_1, x), (p_2, q_2, x)) = \text{Frob}_{K_{p_1 p_2, q_1 q_2}/\mathbb{Q}}(\pi_{z_{\text{Cheb}}}(x)) + g_0$$

with $g_0 \in \mathcal{A}(Y_{z_1} \times Y_{z_2})$ not depending on $\pi_{z_{\text{Cheb}}}(x)$.

Now consider the map $X_{z_{\text{Cheb}}} \to \text{Gal}(M/\mathbb{Q})$ that sends

$$r \mapsto \text{Frob}_{M/\mathbb{Q}}(r).$$

We have that

$$\text{Gal}\left(M / \prod_{p_1, p_2 \in Y_{z_1}} \prod_{q_1, q_2 \in Y_{z_2}} \mathbb{Q}(\sqrt{p_1 p_2}, \sqrt{q_1 q_2})\right) \cong \mathcal{A}(Y_{z_1} \times Y_{z_2})$$

and $\text{Frob}_{M/\mathbb{Q}}(r)$ lands in the above Galois group.

Finishing the proof II

The Chebotarev Density Theorem shows that as r varies we get every element of

$$\mathrm{Gal}\left(M/\prod_{p_1,p_2\in Y_{z_1}}\prod_{q_1,q_2\in Y_{z_2}}\mathbb{Q}(\sqrt{p_1p_2},\sqrt{q_1q_2})\right)$$

equally often.

Finishing the proof II

The Chebotarev Density Theorem shows that as r varies we get every element of

$$\mathrm{Gal}\left(M/\prod_{p_1,p_2\in Y_{z_1}}\prod_{q_1,q_2\in Y_{z_2}}\mathbb{Q}(\sqrt{p_1p_2},\sqrt{q_1q_2})\right)$$

equally often.

Hence varying r, we get every element of

$$g\in\mathcal{A}(Y_{z_1}\times Y_{z_2})$$

equally often.

Finishing the proof II

The Chebotarev Density Theorem shows that as r varies we get every element of

$$\mathrm{Gal}\left(M/\prod_{p_1,p_2\in Y_{z_1}}\prod_{q_1,q_2\in Y_{z_2}}\mathbb{Q}(\sqrt{p_1p_2},\sqrt{q_1q_2})\right)$$

equally often.

Hence varying r, we get every element of

$$g\in\mathcal{A}(Y_{z_1}\times Y_{z_2})$$

equally often.

The combinatorial theorem shows that almost all g are such that all F with $dF=g$ are ϵ-equidistributed.

Finishing the proof II

The Chebotarev Density Theorem shows that as r varies we get every element of

$$\mathrm{Gal}\left(M / \prod_{p_1, p_2 \in Y_{z_1}} \prod_{q_1, q_2 \in Y_{z_2}} \mathbb{Q}(\sqrt{p_1 p_2}, \sqrt{q_1 q_2})\right)$$

equally often.

Hence varying r, we get every element of

$$g \in \mathcal{A}(Y_{z_1} \times Y_{z_2})$$

equally often.

The combinatorial theorem shows that almost all g are such that all F with $dF = g$ are ϵ-equidistributed.

Then F is equidistributed as was to be shown.

Remarks about ℓ^∞

In case $\ell = 2$ our cocycles were valued in $\mathbb{Q}_2/\mathbb{Z}_2$. The correct analogue for $\mathrm{Cl}(K)[\ell^\infty]$ with K cyclic of degree ℓ is $\mathbb{Q}_\ell[\zeta_\ell]/\mathbb{Z}_\ell[\zeta_\ell]$.

Remarks about ℓ^∞

In case $\ell = 2$ our cocycles were valued in $\mathbb{Q}_2/\mathbb{Z}_2$. The correct analogue for $\mathrm{Cl}(K)[\ell^\infty]$ with K cyclic of degree ℓ is $\mathbb{Q}_\ell[\zeta_\ell]/\mathbb{Z}_\ell[\zeta_\ell]$.

In this case one gets reflection principles which compare ℓ^2 Artin pairings. Alternatively one can compare 4 Artin pairings (but with appropriate signs).

Remarks about ℓ^∞

In case $\ell = 2$ our cocycles were valued in $\mathbb{Q}_2/\mathbb{Z}_2$. The correct analogue for $\mathrm{Cl}(K)[\ell^\infty]$ with K cyclic of degree ℓ is $\mathbb{Q}_\ell[\zeta_\ell]/\mathbb{Z}_\ell[\zeta_\ell]$.

In this case one gets reflection principles which compare ℓ^2 Artin pairings. Alternatively one can compare 4 Artin pairings (but with appropriate signs).

If $p \equiv q \equiv 1 \bmod \ell$, there are two cyclic degree ℓ fields that are ramified only at p and q. Their class groups are essentially independent.

Remarks about ℓ^∞

In case $\ell = 2$ our cocycles were valued in $\mathbb{Q}_2/\mathbb{Z}_2$. The correct analogue for $\mathrm{Cl}(K)[\ell^\infty]$ with K cyclic of degree ℓ is $\mathbb{Q}_\ell[\zeta_\ell]/\mathbb{Z}_\ell[\zeta_\ell]$.

In this case one gets reflection principles which compare ℓ^2 Artin pairings. Alternatively one can compare 4 Artin pairings (but with appropriate signs).

If $p \equiv q \equiv 1 \bmod \ell$, there are two cyclic degree ℓ fields that are ramified only at p and q. Their class groups are essentially independent.

Character sums get more intricate since (choosing one character χ_q for each q)

$$\sum_{1 \leq q \leq X} \chi_q(\mathrm{Frob}(p))$$

need not oscillate for a bad choice of characters χ_q.