Formal Verification of BLR PCP

yuxi-zheng

April 28, 2026

Chapter 1

BLR for general finite fields

1.1 BLR over General Finite Fields

Throughout this section, let $q = p^s$ for a prime p and $s \in \mathbb{N}$ with $s \geq 1$. All vectors are in $\mathbb{F}_q^n$, and all expectations are uniform over the indicated finite sets. Let $\omega_p = e^{2\pi i/p}$.

Definition 1.1.1 (Field trace)**.** *The field trace* $\mathrm{Tr} : \mathbb{F}_q \to \mathbb{F}_p$ *is*

$$\mathrm{Tr}(z) := \sum_{i=0}^{s-1} z^{p^i}.$$

Definition 1.1.2 (Additive characters)**.** *For* $\alpha \in \mathbb{F}_q^n$*, define the additive character* $\chi_\alpha : \mathbb{F}_q^n \to \mathbb{C}$ *by*

$$\chi_\alpha(x) := \omega_p^{\mathrm{Tr}(\langle \alpha, x \rangle)},$$

where $\langle \alpha, x \rangle = \sum_{i=1}^n \alpha_i x_i \in \mathbb{F}_q$.

Definition 1.1.3 (Inner product and Fourier coefficient)**.** *For functions* $h_1, h_2 : \mathbb{F}_q^n \to \mathbb{C}$*, define*

$$\langle h_1, h_2 \rangle := \mathbb{E}_{x \in \mathbb{F}_q^n} \left[h_1(x) \overline{h_2(x)} \right].$$

For $h : \mathbb{F}_q^n \to \mathbb{C}$ *and* $\alpha \in \mathbb{F}_q^n$*, define*

$$\hat{h}(\alpha) := \langle h, \chi_\alpha \rangle = \mathbb{E}_{x \in \mathbb{F}_q^n} \left[h(x) \overline{\chi_\alpha(x)} \right].$$

Lemma 1.1.4 (Character orthogonality)**.** *For every* $\alpha, \beta \in \mathbb{F}_q^n$*,*

$$\mathbb{E}_{x \in \mathbb{F}_q^n} \left[\chi_\alpha(x) \overline{\chi_\beta(x)} \right] = \begin{cases} 1 & \text{if } \alpha = \beta, \\ 0 & \text{if } \alpha \neq \beta. \end{cases}$$

Equivalently, $\mathbb{E}_x[\chi_\alpha(x)] = 0$ *for* $\alpha \neq 0$ *and equals* 1 *for* $\alpha = 0$.

Proof. First observe that for every $\alpha, \beta \in \mathbb{F}_q^n$ and every $x \in \mathbb{F}_q^n$,

$$\chi_\alpha(x) \overline{\chi_\beta(x)} = \omega_p^{\mathrm{Tr}(\langle \alpha, x \rangle)} \omega_p^{-\mathrm{Tr}(\langle \beta, x \rangle)} = \omega_p^{\mathrm{Tr}(\langle \alpha - \beta, x \rangle)} = \chi_{\alpha - \beta}(x),$$

where we used the $\mathbb{F}_p$-linearity of the trace map.

If $\alpha = \beta$, then $\alpha - \beta = 0$, so $\chi_{\alpha-\beta}(x) = 1$ for every $x \in \mathbb{F}_q^n$. Hence

$$\mathbb{E}_{x\in\mathbb{F}_q^n}\left[\chi_\alpha(x)\overline{\chi_\beta(x)}\right] = \mathbb{E}_{x\in\mathbb{F}_q^n}[1] = 1.$$

Now suppose $\alpha \neq \beta$. Let $\gamma := \alpha - \beta$. Then $\gamma \neq 0$, so there exists an index j such that $\gamma_j \neq 0$. Fix all coordinates of x except x_j. For the fixed remaining coordinates, the map

$$x_j \mapsto \langle \gamma, x\rangle$$

has the form

$$x_j \mapsto \gamma_j x_j + c$$

for some constant $c \in \mathbb{F}_q$. Since $\gamma_j \neq 0$, multiplication by γ_j is a bijection on $\mathbb{F}_q$, and therefore the affine map $x_j \mapsto \gamma_j x_j + c$ is also a bijection on $\mathbb{F}_q$. Thus, as x_j ranges uniformly over $\mathbb{F}_q$, the value $\langle \gamma, x\rangle$ also ranges uniformly over $\mathbb{F}_q$. Averaging first over x_j and then over the remaining coordinates gives

$$\mathbb{E}_{x\in\mathbb{F}_q^n}\left[\chi_\gamma(x)\right] = \mathbb{E}_{t\in\mathbb{F}_q}\left[\omega_p^{\mathrm{Tr}(t)}\right].$$

It remains to show that this last average is zero. The trace map $\mathrm{Tr} : \mathbb{F}_q \to \mathbb{F}_p$ is a nonzero $\mathbb{F}_p$-linear map, so every fiber of Tr has the same cardinality. Since $\left|\mathbb{F}_q\right| = q$ and $\left|\mathbb{F}_p\right| = p$, each fiber has cardinality q/p. Therefore

$$\begin{aligned}
\mathbb{E}_{t\in\mathbb{F}_q}\left[\omega_p^{\mathrm{Tr}(t)}\right] &= \frac{1}{q}\sum_{t\in\mathbb{F}_q}\omega_p^{\mathrm{Tr}(t)} \\
&= \frac{1}{q}\sum_{r\in\mathbb{F}_p}\sum_{\substack{t\in\mathbb{F}_q \\ \mathrm{Tr}(t)=r}}\omega_p^r \\
&= \frac{1}{q}\sum_{r\in\mathbb{F}_p}\frac{q}{p}\omega_p^r \\
&= \frac{1}{p}\sum_{r\in\mathbb{F}_p}\omega_p^r \\
&= 0,
\end{aligned}$$

because the sum of all p-th roots of unity is zero. Hence, if $\alpha \neq \beta$, then

$$\mathbb{E}_{x\in\mathbb{F}_q^n}\left[\chi_\alpha(x)\overline{\chi_\beta(x)}\right] = 0.$$

Combining the two cases proves the stated orthogonality relation. The equivalent formulation follows by taking $\beta = 0$. □

Lemma 1.1.5 (Fourier inversion and Parseval)**.** *For every function $h : \mathbb{F}_q^n \to \mathbb{C}$,*

$$h(x) = \sum_{\alpha\in\mathbb{F}_q^n}\hat{h}(\alpha)\chi_\alpha(x) \quad \textit{for every } x \in \mathbb{F}_q^n,$$

and

$$\sum_{\alpha\in\mathbb{F}_q^n}\left|\hat{h}(\alpha)\right|^2 = \mathbb{E}_{x\in\mathbb{F}_q^n}\left[|h(x)|^2\right].$$

In particular, if $|h(x)| = 1$ for every x, then $\sum_{\alpha\in\mathbb{F}_q^n}\left|\hat{h}(\alpha)\right|^2 = 1$.

Proof. By Lemma 1.1.4, the additive characters

$$\{\chi_\alpha : \alpha \in \mathbb{F}_q^n\}$$

are orthonormal with respect to the inner product

$$\langle h_1, h_2 \rangle = \mathbb{E}_{x \in \mathbb{F}_q^n} \left[h_1(x) \overline{h_2(x)} \right].$$

Moreover, these characters span the vector space of all complex-valued functions on $\mathbb{F}_q^n$. Indeed, there are exactly q^n characters, and the space of functions $\mathbb{F}_q^n \to \mathbb{C}$ has dimension q^n. Since the characters are nonzero and pairwise orthogonal, they are linearly independent. Hence they form an orthonormal basis.

Therefore every function $h : \mathbb{F}_q^n \to \mathbb{C}$ has a unique expansion in this basis:

$$h = \sum_{\alpha \in \mathbb{F}_q^n} c_\alpha \chi_\alpha$$

for some coefficients $c_\alpha \in \mathbb{C}$. Taking the inner product of both sides with χ_β, we obtain

$$\langle h, \chi_\beta \rangle = \sum_{\alpha \in \mathbb{F}_q^n} c_\alpha \langle \chi_\alpha, \chi_\beta \rangle.$$

By orthonormality, all terms in the sum vanish except the term $\alpha = \beta$, and $\langle \chi_\beta, \chi_\beta \rangle = 1$. Hence

$$\langle h, \chi_\beta \rangle = c_\beta.$$

By definition of the Fourier coefficient,

$$\widehat{h}(\beta) = \langle h, \chi_\beta \rangle.$$

Thus $c_\beta = \widehat{h}(\beta)$ for every $\beta \in \mathbb{F}_q^n$. Therefore

$$h = \sum_{\alpha \in \mathbb{F}_q^n} \widehat{h}(\alpha) \chi_\alpha.$$

Evaluating this identity at $x \in \mathbb{F}_q^n$ gives the Fourier inversion formula

$$h(x) = \sum_{\alpha \in \mathbb{F}_q^n} \widehat{h}(\alpha) \chi_\alpha(x).$$

It remains to prove Parseval's identity. Using the Fourier expansion and orthonormality, we compute

$$\begin{aligned} \mathbb{E}_x |h(x)|^2 &= \langle h, h \rangle \\ &= \left\langle \sum_{\alpha \in \mathbb{F}_q^n} \widehat{h}(\alpha) \chi_\alpha, \sum_{\beta \in \mathbb{F}_q^n} \widehat{h}(\beta) \chi_\beta \right\rangle \\ &= \sum_{\alpha, \beta \in \mathbb{F}_q^n} \widehat{h}(\alpha) \overline{\widehat{h}(\beta)} \langle \chi_\alpha, \chi_\beta \rangle. \end{aligned}$$

Again, by orthonormality, $\langle \chi_\alpha, \chi_\beta \rangle = 0$ when $\alpha \neq \beta$, and $\langle \chi_\alpha, \chi_\alpha \rangle = 1$. Hence the double sum reduces to

$$\mathbb{E}_x |h(x)|^2 = \sum_{\alpha \in \mathbb{F}_q^n} \widehat{h}(\alpha) \overline{\widehat{h}(\alpha)} = \sum_{\alpha \in \mathbb{F}_q^n} |\widehat{h}(\alpha)|^2.$$

This proves Parseval's identity.

Finally, if $|h(x)| = 1$ for every $x \in \mathbb{F}_q^n$, then

$$\mathbb{E}_x |h(x)|^2 = \mathbb{E}_x 1 = 1.$$

Therefore Parseval gives

$$\sum_{\alpha \in \mathbb{F}_q^n} |\hat{h}(\alpha)|^2 = 1.$$

□

Definition 1.1.6 (Fourier expansion of a finite-field-valued function)**.** *Let $f : \mathbb{F}_q^n \to \mathbb{F}_q$. For each $c \in \mathbb{F}_q^\times$, define*

$$\varphi_c(x) := \omega_p^{\mathrm{Tr}(cf(x))}.$$

The Fourier expansion of f is the family

$$\{\varphi_c\}_{c \in \mathbb{F}_q^\times}.$$

Lemma 1.1.7 (Character-sum indicator)**.** *For every $z \in \mathbb{F}_q$,*

$$\mathbb{1}[z = 0] = \frac{1}{q} \sum_{c \in \mathbb{F}_q} \omega_p^{\mathrm{Tr}(cz)}.$$

Consequently, for every $u, v \in \mathbb{F}_q$,

$$\mathbb{1}[u = v] = \frac{1}{q} \sum_{c \in \mathbb{F}_q} \omega_p^{\mathrm{Tr}(c(u-v))}.$$

Proof. Let

$$\psi(z) := \omega_p^{\mathrm{Tr}(z)}$$

be the standard additive character of $\mathbb{F}_q$. We prove that, for every $t \in \mathbb{F}_q$,

$$\mathbb{1}[t = 0] = \frac{1}{q} \sum_{c \in \mathbb{F}_q} \psi(ct).$$

The desired statement follows by taking $t = u - v$.

If $t = 0$, then $ct = 0$ for every $c \in \mathbb{F}_q$, so

$$\frac{1}{q} \sum_{c \in \mathbb{F}_q} \psi(ct) = \frac{1}{q} \sum_{c \in \mathbb{F}_q} 1 = 1.$$

Now suppose $t \neq 0$. Then multiplication by t is a bijection $\mathbb{F}_q \to \mathbb{F}_q$, so

$$\sum_{c \in \mathbb{F}_q} \psi(ct) = \sum_{z \in \mathbb{F}_q} \psi(z).$$

We claim that the latter sum is 0. Let

$$S := \sum_{z \in \mathbb{F}_q} \psi(z).$$

Since $\mathrm{Tr} : \mathbb{F}_q \to \mathbb{F}_p$ is a nonzero $\mathbb{F}_p$-linear map, it is surjective. Hence there exists $a \in \mathbb{F}_q$ such that $\mathrm{Tr}(a) = 1$. Using the bijection $z \mapsto z + a$, we get

$$S = \sum_{z \in \mathbb{F}_q} \psi(z+a) = \sum_{z \in \mathbb{F}_q} \omega_p^{\mathrm{Tr}(z+a)} = \sum_{z \in \mathbb{F}_q} \omega_p^{\mathrm{Tr}(z)} \omega_p^{\mathrm{Tr}(a)} = \omega_p S.$$

Since $\omega_p \neq 1$, this implies $S = 0$. Therefore, when $t \neq 0$,

$$\frac{1}{q} \sum_{c \in \mathbb{F}_q} \psi(ct) = 0.$$

Combining the two cases gives

$$\mathbb{1}[t = 0] = \frac{1}{q} \sum_{c \in \mathbb{F}_q} \omega_p^{\mathrm{Tr}(ct)}.$$

Substituting $t = u - v$, we obtain

$$\mathbb{1}[u = v] = \frac{1}{q} \sum_{c \in \mathbb{F}_q} \omega_p^{\mathrm{Tr}(c(u-v))}.$$

□

Definition 1.1.8 (Relative Hamming distance)**.** *For $f, g : \mathbb{F}_q^n \to \mathbb{F}_q$, define*

$$\delta(f, g) := \Pr_{x \in \mathbb{F}_q^n} [f(x) \neq g(x)].$$

Definition 1.1.9 (Linear functions)**.** *For $\alpha \in \mathbb{F}_q^n$, define $\ell_\alpha : \mathbb{F}_q^n \to \mathbb{F}_q$ by*

$$\ell_\alpha(x) := \langle \alpha, x \rangle.$$

The set of linear functions is

$$\mathcal{LIN} := \left\{ \ell_\alpha \mid \alpha \in \mathbb{F}_q^n \right\}.$$

The distance from $f : \mathbb{F}_q^n \to \mathbb{F}_q$ to linearity is

$$\delta(f, \mathcal{LIN}) := \min_{\alpha \in \mathbb{F}_q^n} \delta(f, \ell_\alpha).$$

Lemma 1.1.10 (Distance formula)**.** *Let $f, g : \mathbb{F}_q^n \to \mathbb{F}_q$. Let $\{\varphi_c\}_{c \in \mathbb{F}_q^\times}$ and $\{\gamma_c\}_{c \in \mathbb{F}_q^\times}$ be their Fourier expansions. Then*

$$\delta(f, g) = 1 - \frac{1}{q} \left(1 + \sum_{c \in \mathbb{F}_q^\times} \langle \varphi_c, \gamma_c \rangle \right).$$

Equivalently,

$$\delta(f, g) = 1 - \frac{1}{q} \left(1 + \sum_{c \in \mathbb{F}_q^\times} \sum_{\alpha \in \mathbb{F}_q^n} \widehat{\varphi_c}(\alpha) \overline{\widehat{\gamma_c}(\alpha)} \right).$$

Proof. By Theorem 1.1.7,

$$\Pr_x[f(x) = g(x)] = \mathbb{E}_x\left[\frac{1}{q}\sum_{c\in\mathbb{F}_q}\omega_p^{\mathrm{Tr}(c(f(x)-g(x)))}\right].$$

The term $c = 0$ contributes $1/q$. For $c \neq 0$,

$$\omega_p^{\mathrm{Tr}(c(f(x)-g(x)))} = \varphi_c(x)\overline{\gamma_c(x)}.$$

Therefore

$$\Pr_x[f(x) = g(x)] = \frac{1}{q}\left(1 + \sum_{c\in\mathbb{F}_q^\times}\langle\varphi_c, \gamma_c\rangle\right),$$

which gives the first formula after using $\delta(f, g) = 1 - \Pr_x[f(x) = g(x)]$. The second formula follows from Fourier inversion and Parseval. □

Lemma 1.1.11 (Fourier expansion of a linear function)**.** *Fix $\alpha \in \mathbb{F}_q^n$ and $c \in \mathbb{F}_q^\times$. Let $\lambda_c(x) := \omega_p^{\mathrm{Tr}(c\ell_\alpha(x))}$. Then*

$$\lambda_c = \chi_{c\alpha}.$$

Equivalently, for every $\beta \in \mathbb{F}_q^n$,

$$\widehat{\lambda_c}(\beta) = \begin{cases} 1 & \text{if } \beta = c\alpha, \\ 0 & \text{if } \beta \neq c\alpha. \end{cases}$$

Proof. For every $x \in \mathbb{F}_q^n$,

$$\lambda_c(x) = \omega_p^{\mathrm{Tr}(c\langle\alpha,x\rangle)} = \omega_p^{\mathrm{Tr}(\langle c\alpha,x\rangle)} = \chi_{c\alpha}(x).$$

The statement about Fourier coefficients follows from Theorem 1.1.4. □

Lemma 1.1.12 (Distance to linearity in Fourier form)**.** *Let $f : \mathbb{F}_q^n \to \mathbb{F}_q$ have Fourier expansion $\{\varphi_c\}_{c\in\mathbb{F}_q^\times}$. Then*

$$\delta(f, \mathcal{LIN}) = 1 - \frac{1}{q}\left(1 + \max_{\alpha\in\mathbb{F}_q^n}\sum_{c\in\mathbb{F}_q^\times}\widehat{\varphi_c}(c\alpha)\right).$$

Moreover, for every $\alpha \in \mathbb{F}_q^n$, the quantity

$$S_\alpha := \sum_{c\in\mathbb{F}_q^\times}\widehat{\varphi_c}(c\alpha)$$

is real and satisfies $-1 \leq S_\alpha \leq q - 1$.

Proof. Apply Theorem 1.1.10 with $g = \ell_\alpha$ and use Theorem 1.1.11. This gives

$$\delta(f, \ell_\alpha) = 1 - \frac{1}{q}\left(1 + \sum_{c\in\mathbb{F}_q^\times}\widehat{\varphi_c}(c\alpha)\right).$$

Taking the minimum over α gives the claimed formula for $\delta(f, \mathcal{LIN})$. For fixed α, the same formula expresses S_α as $q(1 - \delta(f, \ell_\alpha)) - 1$. Hence S_α is real, and since $0 \leq \delta(f, \ell_\alpha) \leq 1$, we get $-1 \leq S_\alpha \leq q - 1$. □

Definition 1.1.13 (Finite-field BLR test)**.** *Given oracle access to $f : \mathbb{F}_q^n \to \mathbb{F}_q$, the finite-field BLR verifier $\mathsf{V}_{\mathsf{BLR}}^f$ samples $a, b \in \mathbb{F}_q^\times$ and $x, y \in \mathbb{F}_q^n$ uniformly and accepts iff*

$$af(x) + bf(y) = f(ax + by).$$

That is,

$$\mathsf{V}_{\mathsf{BLR}}^f = 1 \quad \Longleftrightarrow \quad af(x) + bf(y) = f(ax + by).$$

Lemma 1.1.14 (Completeness)**.** *If $f \in \mathcal{LIN}$, then*

$$\Pr[\mathsf{V}_{\mathsf{BLR}}^f = 1] = 1.$$

Proof. If $f = \ell_\alpha$ for some $\alpha \in \mathbb{F}_q^n$, then for every $a, b \in \mathbb{F}_q^\times$ and $x, y \in \mathbb{F}_q^n$,

$$f(ax + by) = \langle \alpha, ax + by \rangle = a\langle \alpha, x \rangle + b\langle \alpha, y \rangle = af(x) + bf(y).$$

Thus the verifier accepts for every choice of randomness. □

Lemma 1.1.15 (Exact BLR acceptance formula)**.** *Let $f : \mathbb{F}_q^n \to \mathbb{F}_q$ have Fourier expansion $\{\varphi_c\}_{c \in \mathbb{F}_q^\times}$. For each $\alpha \in \mathbb{F}_q^n$, define*

$$S_\alpha := \sum_{c \in \mathbb{F}_q^\times} \widehat{\varphi_c}(c\alpha).$$

Then

$$\Pr[\mathsf{V}_{\mathsf{BLR}}^f = 1] = \frac{1}{q}\left(1 + \frac{1}{(q-1)^2} \sum_{\alpha \in \mathbb{F}_q^n} S_\alpha^3\right).$$

Proof. By Theorem 1.1.7, for fixed a, b, x, y,

$$\mathbb{1}[af(x) + bf(y) = f(ax + by)] = \frac{1}{q} \sum_{c \in \mathbb{F}_q} \omega_p^{\mathrm{Tr}(c(af(x) + bf(y) - f(ax+by)))}.$$

Taking expectation gives

$$\Pr[\mathsf{V}_{\mathsf{BLR}}^f = 1] = \frac{1}{q} + \frac{1}{q}\mathbb{E}_{a,b,x,y}\left[\sum_{c \in \mathbb{F}_q^\times} \varphi_{ca}(x)\varphi_{cb}(y)\varphi_{-c}(ax + by)\right].$$

Expand the three complex-valued functions into their Fourier expansions:

$$\begin{aligned}
&\mathbb{E}_{a,b,x,y}\left[\sum_{c \in \mathbb{F}_q^\times} \varphi_{ca}(x)\varphi_{cb}(y)\varphi_{-c}(ax + by)\right] \\
&= \mathbb{E}_{a,b}\left[\sum_{c \in \mathbb{F}_q^\times} \sum_{\alpha,\beta,\gamma \in \mathbb{F}_q^n} \widehat{\varphi_{ca}}(\alpha)\widehat{\varphi_{cb}}(\beta)\widehat{\varphi_{-c}}(\gamma)\mathbb{E}_{x,y}\left[\chi_\alpha(x)\chi_\beta(y)\chi_\gamma(ax + by)\right]\right].
\end{aligned}$$

Since

$$\chi_\gamma(ax + by) = \chi_{a\gamma}(x)\chi_{b\gamma}(y),$$

Theorem 1.1.4 implies that the inner expectation is 1 exactly when

$$\alpha + a\gamma = 0 \quad \text{and} \quad \beta + b\gamma = 0,$$

and is 0 otherwise. Therefore the last display equals

$$\mathbb{E}_{a,b}\left[\sum_{c\in\mathbb{F}_q^\times}\sum_{\alpha\in\mathbb{F}_q^n}\widehat{\varphi_{ca}}(\alpha)\widehat{\varphi_{cb}}(a^{-1}b\alpha)\widehat{\varphi_{-c}}(-a^{-1}\alpha)\right].$$

Substitute $\alpha = ca\eta$. Then this becomes

$$\mathbb{E}_{a,b}\left[\sum_{c\in\mathbb{F}_q^\times}\sum_{\eta\in\mathbb{F}_q^n}\widehat{\varphi_{ca}}(ca\eta)\widehat{\varphi_{cb}}(cb\eta)\widehat{\varphi_{-c}}(-c\eta)\right].$$

As a, b, c range over $\mathbb{F}_q^\times$, so do ca, cb, and $-c$. Hence this equals

$$\frac{1}{(q-1)^2}\sum_{\eta\in\mathbb{F}_q^n}\left(\sum_{d\in\mathbb{F}_q^\times}\widehat{\varphi_d}(d\eta)\right)^3 = \frac{1}{(q-1)^2}\sum_{\eta\in\mathbb{F}_q^n}S_\eta^3.$$

Substituting into the expression for $\Pr[\mathsf{V}^f_{\mathsf{BLR}} = 1]$ proves the claim. □

Lemma 1.1.16 (Second moment bound)**.** *With S_α as in Theorem 1.1.15,*

$$\sum_{\alpha\in\mathbb{F}_q^n}S_\alpha^2 \le (q-1)^2.$$

Proof. Expanding the square gives

$$\sum_{\alpha\in\mathbb{F}_q^n}S_\alpha^2 = \sum_{a,b\in\mathbb{F}_q^\times}\sum_{\alpha\in\mathbb{F}_q^n}\widehat{\varphi_a}(a\alpha)\widehat{\varphi_b}(b\alpha).$$

For fixed $a, b \in \mathbb{F}_q^\times$, Cauchy–Schwarz and Theorem 1.1.5 give

$$\left|\sum_{\alpha\in\mathbb{F}_q^n}\widehat{\varphi_a}(a\alpha)\widehat{\varphi_b}(b\alpha)\right| \le \left(\sum_{\alpha\in\mathbb{F}_q^n}|\widehat{\varphi_a}(a\alpha)|^2\right)^{1/2}\left(\sum_{\alpha\in\mathbb{F}_q^n}|\widehat{\varphi_b}(b\alpha)|^2\right)^{1/2} = 1.$$

The equality uses that multiplication by a and by b permutes $\mathbb{F}_q^n$, and that $|\varphi_a(x)| = |\varphi_b(x)| = 1$ for every x. Summing over the $(q-1)^2$ choices of (a, b) gives the result. □

Theorem 1.1.17 (Soundness of the finite-field BLR test)**.** *For every function $f : \mathbb{F}_q^n \to \mathbb{F}_q$,*

$$\Pr[\mathsf{V}^f_{\mathsf{BLR}} = 0] \ge \delta(f, \mathcal{LIN}).$$

Equivalently,

$$\Pr[\mathsf{V}^f_{\mathsf{BLR}} = 1] \le 1 - \delta(f, \mathcal{LIN}).$$

Proof. Let S_α be as in Theorem 1.1.15, and let

$$M := \max_{\alpha\in\mathbb{F}_q^n}S_\alpha.$$

By Theorem 1.1.12,

$$1 - \delta(f, \mathcal{LIN}) = \frac{1}{q}(1 + M).$$

By Theorem 1.1.12, each S_α is real and $S_\alpha \leq M$. Therefore $S_\alpha^3 \leq M S_\alpha^2$ for every α, because $S_\alpha^2 \geq 0$. Using Theorem 1.1.15 and Theorem 1.1.16,

$$\begin{aligned}
\Pr[\mathsf{V}_{\mathsf{BLR}}^f = 1] &= \frac{1}{q}\left(1 + \frac{1}{(q-1)^2}\sum_{\alpha \in \mathbb{F}_q^n} S_\alpha^3\right) \\
&\leq \frac{1}{q}\left(1 + \frac{M}{(q-1)^2}\sum_{\alpha \in \mathbb{F}_q^n} S_\alpha^2\right) \\
&\leq \frac{1}{q}(1+M) \\
&= 1 - \delta(f, \mathcal{LIN}).
\end{aligned}$$

Taking complements gives $\Pr[\mathsf{V}_{\mathsf{BLR}}^f = 0] \geq \delta(f, \mathcal{LIN})$. □

Chapter 2

Gowers Hatami theorem

2.1 Preliminaries

Definition 2.1.1 (σ inner product.)**.** *The σ inner product between matrices A and B is defined as*

$$\langle A, B\rangle_\sigma = \mathrm{Tr}(A^* B\sigma), \tag{2.1}$$

where $\sigma \geq 0$ and A^* denotes conjugate-transpose.

Definition 2.1.2 ((ϵ, σ)-representation.)**.** *Given a finite group G, an integer $d \geq 1, \varepsilon \geq 0$, and a d-dimensional positive semidefinite matrix σ with trace 1 , an (ε, σ)-representation of G is a map $f : G \to U_d(\mathbb{C})$, to the $d \times d$ unitary matrices, such that*

$$\mathbb{E}_{x,y\in G}\mathfrak{R}\left(\left\langle f(x)^* f(y), f\left(x^{-1}y\right)\right\rangle_\sigma\right) \geq 1 - \varepsilon, \tag{2.2}$$

where $\mathfrak{R}$ denotes taking real part of the inner product.

Proposition 2.1.3. *Let G be a finite group, and let $f, f_2 : G \to U(n)$ be functions into the unitary matrices. Then*

$$\mathbb{E}_{x\in G}\|f(x) - f_2(x)\|_\sigma^2 \leq 2\varepsilon \quad \iff \quad \mathbb{E}_{x\in G}\mathfrak{R}(\langle f(x), f_2(x)\rangle_\sigma) \geq 1 - \varepsilon.$$

Proof. For unitary matrices A, B, we have

$$\|A - B\|_\sigma^2 = 2 - 2\mathfrak{R}\langle A, B\rangle_\sigma. \tag{2.3}$$

Since $\mathbb{E}$ is linear, this proves the proposition. □

TODO:

- Relation to classical BLR test

2.2 Representation theory

Definition 2.2.1 (Unitary Representation)**.** *A* unitary representation *of G is a representation to unitary matrices $\rho : G \to U(V)$.*

Definition 2.2.2 (Regular representation)**.** *Let $R : G \to \mathbb{C}[G]$ be a regular representation where $\{|g\rangle, g \in G\}$ forms a basis of $\mathbb{C}[G]$. The representation is given by*

$$R(x)|g\rangle = |xg\rangle. \tag{2.4}$$

It is possible to decompose any representation of a finite group into direct sums over irreps.

Theorem 2.2.3 (Maschke's theorem)**.** *Let G be a finite group and let $\rho : G \to \mathrm{GL}(V)$ be a finite-dimensional representation over $\mathbb{C}$. Then ρ is completely reducible. In particular, there exists a decomposition*

$$\rho \cong \bigoplus_m r_m \, \rho_m, \tag{2.5}$$

where $\{\rho_m\}$ is a set of inequivalent irreducible representations of G, and $r_m \in \mathbb{Z}^+$ are the multiplicities.

Proof sketch. Maschke's theorem is partially formalized in `Mathlib.RepresentationTheory.Maschke` but incomplete. Jonathan's team is formalizing this. □

Proposition 2.2.4 (Decomposition of the regular representation)**.** *Let $R : G \to \mathrm{GL}(\mathbb{C}[G])$ be the regular representation of a finite group G. Then*

$$R \cong \bigoplus_{\rho \in \widehat{G}} d_\rho \, \rho, \tag{2.6}$$

where $\widehat{G}$ is a complete set of inequivalent irreducible representations of G, and $d_\rho = \dim(V_\rho)$ is the dimension of ρ.

Proof sketch. This can be proven using Maschke's theorem in 2.2.3 to decompose into irreps with multiplicity. Then use character orthogonality theorem in mathlib `FDRep.char_orthonormal` to show the multiplicity equals irrep dimension. A more formal statement is given by the Peter-Weyl theorem. □

Proposition 2.2.5 (Character of regular representation.)**.** *Let G be a finite group and $\sum_\rho$ denotes summing over the complete set of inequivalent irreps $\hat{G}$*

$$\sum_{\rho \in \hat{G}} d_\rho \, \mathrm{Tr}(\rho(x)) = |G| \delta_{x,e}. \tag{2.7}$$

Proof sketch. The proof uses decomposition of regular representation and definition of character. □

Definition 2.2.6 (Group fourier transform)**.** *Let $f : G \to U_d(\mathbb{C})$ be a map and $\rho : G \to U_{d_\rho}(\mathbb{C})$ be a unitary irrep. The fourier transform of f at the representation ρ is denoted by $\hat{f}$:*

$$\hat{f}(\rho) = \mathbb{E}_{x \in G} f(x) \otimes \overline{\rho(x)}, \tag{2.8}$$

where $\overline{\rho(x)}$ denotes complex conjugate of $\rho(x)$.

2.3 Gowers Hatami Theorem

Theorem 2.3.1 (Gowers-Hatami)**.** *Let G be a finite group, $\varepsilon \geq 0$, and $f : G \to U_d(\mathbb{C})$ an (ε, σ)-representation of G. Then there exists a $d' \geq d$, an isometry $V : \mathbb{C}^d \to \mathbb{C}^{d'}$, and a representation $g : G \to U_{d'}(\mathbb{C})$ such that*

$$\mathbb{E}_{x \in G} \left\| f(x) - V^* g(x) V \right\|_\sigma^2 \leq 2\varepsilon. \tag{2.9}$$

Proof sketch. The full proof can be found in the lecture notes Theorem 2.3 [**?**]. In particular, the proof is constructive. The isometry is defined as $V : \mathbb{C}^d \to \mathbb{C}^d \otimes \left(\oplus_\rho \mathbb{C}^{d_\rho} \otimes \mathbb{C}^{d_\rho} \right)$ by

$$Vu = \bigoplus_\rho d_\rho^{1/2} \sum_{i=1}^{d_\rho} \left(\hat{f}(\rho) \left(u \otimes e_i \right) \right) \otimes e_i. \tag{2.10}$$

And the exact representation is defined as

$$g(x) = \bigoplus_\rho \left(I_d \otimes I_{d_\rho} \otimes \rho(x) \right). \tag{2.11}$$

The proof requires the following two ingredients:

1. V is an isometry:
$$V^* V = \mathbb{I}_d \tag{2.12}$$
2. The isometry "averages" over group multiplication. For any $x \in G$,
$$V^* g(x) V = \mathbb{E}_z f(z)^* f(zx). \tag{2.13}$$

Both ingredients follow from the key identity over the regular representation in Eq. (2.7). □

Theorem 2.3.2 (Gowers-Hatami-2)**.** *Let G be a finite group, $\varepsilon \geq 0$, and $\rho : G \to U(\mathcal{H})$ an (ε, σ)-representation of G on space $\mathcal{H} = \mathbb{C}^d$. Then there exists an isometry $V : \mathcal{H} \to \mathcal{H}'$ to a different space $\mathcal{H}'$, and a representation $\rho' : G \to \mathcal{H}'$ such that*

$$\mathbb{E}_{x \in G} \left\| \rho(x) - V^* \rho'(x) V \right\|_\sigma^2 \leq 2\varepsilon. \tag{2.14}$$

Proof. A different proof of the Gowers-Hatami theorem is given in M. de la Salle's notes [**?**]. Here $\mathcal{H}' = L(G, \mathcal{H})$ is the space of functions $f : G \to \mathcal{H}$. The isometry is given by the action of the approximate representation on a state $u \in \mathcal{H}$ as

$$V : \quad \mathcal{H} \to L(G, \mathcal{H}), \tag{2.15}$$
$$V(u) : \quad G \to \mathcal{H}, \quad x \mapsto \rho(x)(u), \forall x \in G. \tag{2.16}$$

The inverse map V^* is given by the group average

$$V^* : \quad L(G, \mathcal{H}) \to \mathcal{H}, \tag{2.17}$$
$$V^*(f) \quad = \mathbb{E}_{x \in G} \left[\rho^*(x) f(x) \right]. \tag{2.18}$$

The exact representation is given by the right regular representation on $L(G, \mathcal{H})$:

$$\rho' : \quad G \to \mathrm{End}(L(G, \mathcal{H})), \tag{2.19}$$
$$(\rho'(x) f)(y) \quad = f(yx), \quad \forall x, y \in G. \tag{2.20}$$

V is an isometry because

$$V^*V(u) = \mathbb{E}_{x\in G}\left[\rho^*(x)\rho(x)(u)\right] = u. \tag{2.21}$$

The isometry "averages" over group multiplication because

$$\begin{aligned} V^*\rho'(x)V(u) &= \mathbb{E}_{y\in G}\left[\rho^*(y)(\rho'(x)\rho(y))(u)\right] \\ &= \mathbb{E}_{y\in G}\left[\rho^*(y)(\rho(yx)(u))\right]. \end{aligned} \tag{2.22}$$

The rest of the proof follows by expanding the σ-norm, bounding the norm of $\mathbb{E}_{x\in G}V^*\rho'(x)V$ and applying the definition of (ε,σ)-representation. In particular, we have

$$\begin{aligned} & \mathbb{E}_{x\in G}\left\|\rho(x) - V^*\rho'(x)V\right\|_\sigma^2 \\ = \;& \mathbb{E}_{x\in G}\|\rho(x)\|_\sigma^2 + \mathbb{E}_{x\in G}\|V^*\rho'(x)V\|_\sigma^2 - 2\mathbb{E}_{x\in G}\Re\langle\rho(x), V^*\rho'(x)V\rangle_\sigma \end{aligned} \tag{2.23}$$

Because ρ is unitary, $\mathbb{E}_{x\in G}\|\rho(x)\|_\sigma^2 = 1$. For the second term, since ρ' is unitary and V is an isometry,

$$\begin{aligned} & \mathbb{E}_{x\in G}\|V^*\rho'(x)V\|_\sigma^2 \\ = \;& \mathbb{E}_{x\in G}\mathrm{Tr}\left[V^*\rho'^*(x)VV^*\rho'(x)V\sigma\right] \\ = \;& \mathbb{E}_{x,y,z\in G}\mathrm{Tr}\left[\rho^*(yx)\rho(y)\rho^*(z)\rho(zx)\sigma\right] \end{aligned} \tag{2.24}$$

Because ρ is unitary the product $U(x,y,z) := \rho^*(yx)\rho(y)\rho^*(z)\rho(zx)$ is again a unitary operator, the above expression is upper bounded by Holder's inequality as

$$\begin{aligned} & \mathbb{E}_{x,y,z\in G}\mathrm{Tr}\left[U(x,y,z)\sigma\right] \\ \leq \;& \mathbb{E}_{x,y,z\in G}\|U(x,y,z)\|_\infty\|\sigma\|_1 = 1. \end{aligned} \tag{2.25}$$

Finally, using the isometry average property in Eq. 2.22 and the definition of (ε,σ)-representation, we have

$$\begin{aligned} & \mathbb{E}_{x\in G}\Re\langle\rho(x), V^*\rho'(x)V\rangle_\sigma, \\ = \;& \mathbb{E}_{x,y\in G}\Re\langle\rho(x), \rho^*(y)\rho(yx)\rangle_\sigma, \\ \geq \;& 1-\varepsilon. \end{aligned} \tag{2.26}$$

Therefore using the bounds in Eq. 2.25 and Eq. 2.26, we have

$$\mathbb{E}_{x\in G}\left\|\rho(x) - V^*\rho'(x)V\right\|_\sigma^2 \leq 2 - 2(1-\varepsilon) = 2\varepsilon. \tag{2.27}$$

This completes the proof. □

Chapter 3

Exponential-length PCP

Definition 3.0.1. *A system of m quadratic equations in n variables over a field $\mathbb{F}$ is a list of polynomials $p_1, \ldots, p_m \in \mathbb{F}[x_1, \ldots, x_n]$ where each p_i has total degree at most 2.*

$$\mathrm{QESAT}(\mathbb{F}, n) := \{(p_1, \ldots, p_m) \mid \exists a_1, \ldots, a_n \in \mathbb{F},\ \forall i \in [m],\ p_i(a_1, \ldots, a_n) = 0\}.$$

For example, $(x + 1, xy + z) \in \mathrm{QESAT}(\mathbb{F}_2, 3)$.

Definition 3.0.2. *A* PCP verifier *is a probabilistic oracle Turing machine V with query access to a function $\pi : [\ell(|x|)] \to \Sigma$.*

Definition 3.0.3. *A language $L \subseteq \{0,1\}^*$ is in $\mathrm{PCP}[\varepsilon_c, \varepsilon_s, \Sigma, \ell, q, r]$ if there exists a polynomial-time PCP verifier V such that for every $x \in \{0,1\}^*$, V makes at most $q(|x|)$ queries to the proof oracle, uses at most $r(|x|)$ bits of randomness, and the following holds:*

- *Completeness: If $x \in L$, then $\exists \pi \in \Sigma^{\ell(|x|)}$, $\Pr[V^{\pi}(x) = 1] \geq 1 - \varepsilon_c$.*
- *Soundness: If $x \notin L$, then $\forall \tilde{\pi} \in \Sigma^{\ell(|x|)}$, $\Pr\left[V^{\tilde{\pi}}(x) = 1\right] \leq \varepsilon_s$.*

The following theorem is the main goal of this chapter.

Theorem 3.0.4.

$$\mathrm{QESAT}(\mathbb{F}_2, n) \in \mathrm{PCP}[\varepsilon_c = 0, \varepsilon_s = 1/2, \Sigma = \mathbb{F}_2, \ell = \exp(|x|), q = O(1), r = |x|^{O(1)}].$$

Proof. □

Definition 3.0.5. *A* LPCP verifier *is a probabilistic oracle Turing machine V with query access to a linear function $\langle \pi, \cdot \rangle : \Sigma^{\ell(|x|)} \to \Sigma$.*

Definition 3.0.6. *A language $L \subseteq \{0,1\}^*$ is in $\mathrm{LPCP}[\varepsilon_c, \varepsilon_s, \Sigma, \ell, q, r]$ if there exists a polynomial-time LPCP verifier V such that for every $x \in \{0,1\}^*$, V makes at most $q(|x|)$ queries to the linear proof oracle, uses at most $r(|x|)$ bits of randomness, and the following holds:*

- *Completeness: If $x \in L$, then $\exists \pi \in \Sigma^{\ell(|x|)}$, $\Pr\left[V^{\langle \pi, \cdot \rangle}(x) = 1\right] \geq 1 - \varepsilon_c$.*
- *Soundness: If $x \notin L$, then $\forall \tilde{\pi} \in \Sigma^{\ell(|x|)}$, $\Pr\left[V^{\langle \tilde{\pi}, \cdot \rangle}(x) = 1\right] \leq \varepsilon_s$.*

3.1 Linear PCP for linear equations

Definition 3.1.1. *For a field $\mathbb{F}$ and parameters $m, n \in \mathbb{N}$, we define the language*

$$\mathrm{LINEQ}(\mathbb{F}, m, n) := \{(M, c) \in \mathbb{F}^{m \times n} \times \mathbb{F}^m \mid \exists b \in \mathbb{F}^n,\ Mb = c\}.$$

Definition 3.1.2. *Let $V^{\langle b, \cdot \rangle}_{\mathrm{LINEQ}(\mathbb{F},m,n)}(M, c)$ be the LPCP verifier defined as follows:*

1. *Sample $r \leftarrow \mathbb{F}^m$.*
2. *Query $b \in \mathbb{F}^n$ at $u := M^\top r \in \mathbb{F}^n$.*
3. *Accept if and only if $\langle b, u \rangle = \langle c, r \rangle$.*

Theorem 3.1.3.

$$\mathrm{LINEQ}(\mathbb{F}, m, n) \in \mathrm{LPCP}\left[\varepsilon_c = 0, \varepsilon_s = 1/|\mathbb{F}|, \Sigma = \mathbb{F}, \ell = |x|, q = 1, r = m \log |\mathbb{F}|\right].$$

Proof. Consider the LPCP verifier $V^{\langle b, \cdot \rangle}_{\mathrm{LINEQ}(\mathbb{F},m,n)}(M, c)$.
Completeness: If $Mb = c$, then for every $r \in \mathbb{F}^m$, we have

$$\langle b, u \rangle = b^\top (M^\top r) = (Mb)^\top r = \langle c, r \rangle.$$

Soundness: If $Mb \neq c$, then

$$\begin{aligned} \Pr_{r \leftarrow \mathbb{F}^m}\left[\langle b, u \rangle = \langle c, r \rangle\right] &= \Pr_{r \leftarrow \mathbb{F}^m}\left[\langle Mb, r \rangle = \langle c, r \rangle\right] \\ &= \Pr_{r \leftarrow \mathbb{F}^m}\left[\sum_{i=1}^{m} (Mb - c)_i \cdot r_i = 0\right] \leq 1/|\mathbb{F}|, \end{aligned}$$

where the last inequality follows from the Schwartz-Zippel lemma. □

3.2 Linear PCP for tensor checks

Definition 3.2.1. *For a field $\mathbb{F}$, vectors $a \in \mathbb{F}^n$ and $b \in \mathbb{F}^m$, the tensor product $a \otimes b \in \mathbb{F}^{n \times m}$ is the matrix defined by*

$$(a \otimes b)_{i,j} := a_i \cdot b_j \quad \forall i \in [n],\ j \in [m].$$

We write $\mathrm{flat}(a \otimes b) \in \mathbb{F}^{n \cdot m}$ for the row-concatenation of $a \otimes b$.

For our purposes, we would love to test to check if $\mathrm{flat}(a \otimes a) = b$

Definition 3.2.2. *For a field $\mathbb{F}$ and $n \in \mathbb{N}$, define the tensor test language*

$$\mathrm{TENSORQ}(\mathbb{F}, n) := \left\{(a, b) \in \mathbb{F}^n \times \mathbb{F}^{n^2} \mid b = \mathrm{flat}(a \otimes a)\right\}.$$

Theorem 3.2.3. *For every finite field $\mathbb{F}$ and $n \in \mathbb{N}$,*

$$\mathrm{TENSORQ}(\mathbb{F}, n) \in \mathrm{LPCP}\left[\varepsilon_c = 0,\ \varepsilon_s = \frac{2|\mathbb{F}| - 1}{|\mathbb{F}|^2},\ \Sigma = \mathbb{F},\ \ell = n + n^2,\ q = 2,\ r = 2n \cdot \log(|\mathbb{F}|)\right].$$

Proof. Consider the following LPCP verifier $V^{\langle a, \cdot \rangle, \langle b, \cdot \rangle}$ proceeds as follows:

1. Sample $s, t \leftarrow \mathbb{F}^n$.

2. Query a at s and at t, obtaining $\langle a, s\rangle$ and $\langle a, t\rangle$.

3. Query b at $\mathrm{flat}(s \otimes t)$, obtaining $\langle b, \mathrm{flat}(s \otimes t)\rangle$.

4. Check if $\langle b, \mathrm{flat}(s \otimes t)\rangle = \langle a, s\rangle \cdot \langle a, t\rangle$.

Completeness. Suppose $b = \mathrm{flat}(a \otimes a)$. Then $\forall s, t \in \mathbb{F}^n$,

$$\begin{aligned}\langle b,\, \mathrm{flat}(s \otimes t)\rangle &= \langle \mathrm{flat}(a \otimes a),\, \mathrm{flat}(s \otimes t)\rangle = \sum_{i,j \in [n]} a_i a_j s_i t_j \\ &= \Big(\sum_{i \in [n]} a_i s_i\Big) \cdot \Big(\sum_{j \in [n]} a_j t_j\Big) = \langle a, s\rangle \cdot \langle a, t\rangle,\end{aligned}$$

Soundness. Suppose $b \neq \mathrm{flat}(a \otimes a)$, i.e., there exists $i^*, j^* \in [n]$ such that $b_{i^* j^*} \neq a_{i^*} \cdot a_{j^*}$. For each $i \in [n]$ define the linear polynomial $p_i(t) := \sum_{j \in [n]} (b_{ij} - a_i a_j)\, t_j$. The check can be rewritten as

$$\langle b, \mathrm{flat}(s \otimes t)\rangle - \langle a, s\rangle\langle a, t\rangle = \sum_{i \in [n]} \sum_{j \in [n]} (b_{ij} - a_i a_j)\, s_i t_j = \sum_{i \in [n]} p_i(t)\, s_i.$$

Immediate application of Polynomial Identity Testing yields a lower bound of $1 - \frac{2}{|\mathbb{F}|}$ but we can do better. Since $b_{i^* j^*} \neq a_{i^*} a_{j^*}$, the polynomial p_{i^*} is nonzero, so by the Schwartz–Zippel lemma applied to t,

$$\Pr_t[p_{i^*}(t) \neq 0] \geq 1 - \tfrac{1}{|\mathbb{F}|}.$$

Conditioned on $p_{i^*}(t) \neq 0$, the expression $\sum_i p_i(t)\, s_i$ is a nonzero linear polynomial in s, so by the Schwartz–Zippel lemma applied to s,

$$\Pr_{s \leftarrow \mathbb{F}^n}\Big[\sum_i p_i(t)\, s_i \neq 0 \;\Big|\; p_{i^*}(t) \neq 0\Big] \geq 1 - \tfrac{1}{|\mathbb{F}|}.$$

Hence

$$\Pr_{s,t}[\text{verifier rejects}] \;\geq\; \Big(1 - \tfrac{1}{|\mathbb{F}|}\Big)^2,$$

and therefore

$$\Pr_{s,t}[\text{verifier accepts}] \;\leq\; 1 - \Big(1 - \tfrac{1}{|\mathbb{F}|}\Big)^2 = \frac{2|\mathbb{F}| - 1}{|\mathbb{F}|^2}. \qquad \square$$

Corollary 3.2.4.

$$\mathrm{TENSORQ}(\mathbb{F}_2, n) \in \mathrm{LPCP}\Big[\varepsilon_c = 0,\ \varepsilon_s = \frac{3}{4},\ \Sigma = \mathbb{F}_2,\ \ell = n + n^2,\ q = 2,\ r = 2\log(2) \cdot n\Big].$$

Proof. Immediate. $\square$

3.3 Linear PCP to PCP