Chapter 9

Gaussian operators over finite fields

[Draft] 30.06.07 /users/neretin/public_html/lectures/lectures.htm

The main construction of this chapter is a correspondence between Gaussian operators and linear relations over finite fileds, it is a subject of Section 9.3; this construction is almost independent on Sections 9.1–9.2; only some detail require manipulations with Gauss sums (Section 9.2). The last section on numerical Fourier transform is a digression.

In this chapter, p is a prime, $\boxed{p \neq 2}$.

9.1 Quadratic forms over finite fields

1.1. Notation. Let p be a prime integer, $p \neq 2$. Denote by $\mathbb{F}_p$ the field with p elements. We identify $\mathbb{F}_p$ with the field of residues modulo p. By $\mathbb{F}_p^* = \mathbb{F}_p \setminus 0$ denote the multiplicative group of $\mathbb{F}_p$. Recall that this group is cyclic,

$$\mathbb{F}_p^* \simeq \mathbb{Z}_{p-1}$$

Consider the subgroup $(\mathbb{F}_p^*)^2 \subset \mathbb{F}_p^*$ of squares, i.e., elements x^2, where $x \in \mathbb{F}_p^*$. Since $(p-1)$ is even, it follows that the quotient group $\mathbb{F}_p^*/(\mathbb{F}_p^*)^2$ consists of two elements. Recall that the *Legendre symbol* (we also use an alternative notation η) is defined by

$$\eta(y) = \left(\frac{y}{p}\right) := \begin{cases} 1 & \text{if } y = x^2 \\ -1 & \text{if } y \text{ is not a square} \end{cases} \tag{1.1}$$

If $\eta(y) = 1$, we say that y is a *quadratic residue*, otherwise, it is a *quadratic nonresidue*.

By definition, the Legendre symbol is a homomorphism from the group $\mathbb{Z}_{p-1}$ to its quotient $\mathbb{Z}_2$.

Therefore, the Legendre symbol is a homomorphism $\mathbb{F}_p^*/(\mathbb{F}_p^*)^2 \to \mathbb{Z}_2$,

$$\left(\frac{y_1y_2}{p}\right) = \left(\frac{y_1}{p}\right)\left(\frac{y_2}{p}\right) \tag{1.2}$$

Also,

$$\left(\frac{x}{p}\right) = x^{(p-1)/2} \tag{1.3}$$

Here we evaluate the power of x in $\mathbb{F}_p$, evidently, this power equals ± 1.

Obviously,

$$\left(\frac{-1}{p}\right) = \left\{\begin{matrix} 1 & \text{if } p = 4k+1 \\ -1 & \text{if } p = 4k+3 \end{matrix}\right\} = (-1)^{(p-1)/2} \tag{1.4}$$

Sometimes, it is convenient to extend η to the whole field $\mathbb{F}_p$ by the assumption $\eta(0) = 0$.

Problem 1.1 Convince yourself that (1.2)–(1.3) are obvious.

1.2. Quadratic forms. Preliminary remarks. Let V be a finite dimensional linear space other $\mathbb{F}_p$. We define symmetric bilinear forms on V in the usual way[1] (see Subsection 3.1.1). For a bilinear form $H(x, y)$, define the quadratic form $B(x) := H(x, x)$. The form H can be reconstructed from B by

$$B(x) := \frac{1}{2}(B(x+y, x+y) - B(x,x) - B(y,y)) \tag{1.5}$$

Lemma 1.1 *a) Each symmetric bilinear form can be reduced to*

$$B(x) = \sum a_j x_j^2 \tag{1.6}$$

in some basis.

b) Let $B(z, z) = a \neq 0$. Then B can be reduced to

$$B(x) = ax_1^2 + \sum_{k,l\geqslant 2} b_{kl}x_kx_l$$

c) Let $B(z, z) = 0$ for some $z \neq 0$. Then B can be reduced to

$$B(x) = x_1x_2 + \sum_{k,l\geqslant 3} b_{kl}x_kx_l$$

[1] For $p = 2$, we meet an obstacle, because $+1 = -1$; hence symmetric and skew symmetric forms are the same. However quadratic forms and bilinear forms are different objects, as we seen above above in Subsections 8.3.1–8.3.2

PROOFS are usual.

1.3. Quadratic forms. Classification. Consider a nondegenerate quadratic form

$$xQx^t = \sum q_{kl} x_k x_l$$

We define its *discriminant* $\mathrm{Dis}(Q)$ as the determinant $\det(Q)$ regarded as an element of $\mathbb{F}_p{}^*/(\mathbb{F}_p{}^*)^2$,

$$\mathrm{Dis}\, Q := \left(\frac{\det Q}{p}\right)$$

Observation 1.2 *The discriminant is an invariant of a quadratic form.*

PROOF. A linear transformation to $x \mapsto xU$ takes Q to $Q \to UQU^t$. □

The following theorem claims that this invariant is unique.

Theorem 1.3 *Each nondegenerate quadratic form can be reduced to one of the following forms*

$$x_1^2 + \cdots + x_{n-1}^2 + x_n^2, \tag{1.7}$$

$$x_1^2 + \cdots + x_{n-1}^2 + rx_n^2, \tag{1.8}$$

where r is a quadratic nonresidue (i.e., $\eta(r) = -1$).

PROOF. Substitute $x_j \mapsto \alpha_j x_j$ in (1.6), where a_j are arbitrary constants. Then $a_j \mapsto a_j \alpha_j^2$. Therefore our form can be reduced to

$$\sum_{j \leqslant t} x_j^2 + r \sum_{j > t} x_j^2 \tag{1.9}$$

Now the theorem follows from the next lemma

Lemma 1.4 *The binary forms*

$$T_1(x) = x_1^2 + x_2^2, \qquad T_2(x) = rx_1^2 + rx_2^2$$

are equivalent

PROOF. First, $1 + x_2^2$ has $(p+1)/2$ values. Also, $r + rx_2^2$ has $(p+1)/2$ values. Hence there are nonzero u, $v \in \mathbb{F}_p^2$ such that $T_1(u) = T_2(v)$. There are two cases

1) A joint value is 0. By Lemma 1.1c), both forms can be reduced to $y_1 y_2$.

2) A joint value is $a \neq 0$. By Lemma 1.1b), our forms can be reduced to

$$T_1(z) = ay_1^2 + b_1 y_2^2, \qquad T_2(z) = ay_1^2 + b_2 y_2^2$$

Since $\mathrm{Dis}\, T_1 = \mathrm{Dis}\, T_2$, then $b_1 = b_2$ as elements of $\mathbb{F}_p^*/(\mathbb{F}_p^*)^2$. □

1.4. Another canonical form.

Theorem 1.5 *Each nondegenerate quadratic form of* $(2k+1)$ *variables can be reduced to*

$$x_1x_2 + \cdots + x_{2k-1}x_{2k} + s \cdot x_{2k+1}^2$$

where s *is a parameter (quadratic residue or non-residue).*

Each form of $2k$ *variables can be reduced to*

$$x_1x_2 + \cdots + x_{2k-3}x_{2k-2} + x_{2k-1}^2 + s \cdot x_{2k}^2$$

Lemma 1.6 *a) Let* $n \geqslant 3$. *Then each non-degenerate form on* $\mathbb{F}_p^n$ *has an isotropic vector.*

b) Let $n = 2$. *Then the set of values of a non-degenerate form includes all the nonzero numbers.*

PROOF OF THE LEMMA. a) Let $\varphi(x) = a_1x_1^2 + a_2x_2^2 + a_3x_3^2$ where a_j are 1 or r. Let $a_i + a_j = 0$ for some i, j; say $a_1 + a_2 = 0$. Then the vector $(1, 1, 0)$ is isotropic.

Let $p = 4k + 1$. Two of numbers a_i, a_j must be equal, say $a_1 = a_2 =: c$. Since (-1) is a quadratic residue,

$$c(x_1^2 + x_2^2) + a_3x_3^2 \sim c(x_1^2 - x_2^2) + a_3x_3^2$$

and the vector $(1, 1, 0)$ is isotropic.

Let $p = 4k + 3$. Then (-1) is a quadratic non-residue. If both 1 and -1 are present among $a_j \in \mathbb{F}_p/(\mathbb{F}_p^*)2$, then, obviously, there is an isotropic vector. Otherwise,

$$a(x_1^2 + x_2^2 + x_3^2) \sim a(-x_1^2 - x_2^2 + x_3^2)$$

and we again get an isotropic vector $(0, 1, 1)$.

b) It suffices to show that the equation $a_1x_1^2 + a_2y_2^2 = c$ has a non-zero solution for each $c \neq 0$. In other words, we must show that the form $\varphi(x_1, x_2, y) := a_1x_1^2 + a_2x_2^2 - cy^2$ has an isotropic vector (ξ, η, θ) with $\theta \neq 0$. By the statement a), this form has an isotropic vector. If $\theta = 0$, then the form $a_1x_1^2 + a_2x_2^2$ itself has an isotropic vector. Hence (see Lemma 2.1.3) it can be reduced to the form $2x_1x_2$, and the latter form represents all values. □

PROOF OF THEOREM 1.5. If $n \geqslant 3$, then there is an isotropic vector. We apply Lemma 2.1.3 and repeat the second proof of Theorem 2.1.9.

1.5. Symplectic group. We define skew-symmetric bilinear forms over $\mathbb{F}_p$ in the usual way. As above (Theorem 3.1.1), non-degenerate forms exist only on even-dimensional spaces; all the non-degenerate forms on a $2n$-dimensional space are equivalent to the form $\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$.

We denote by $\mathrm{Sp}(2n, \mathbb{F}_p)$ (*symplectic group*) the group of all linear transformations preserving this form.

9.2 The Fourier transform and Gauss sums

Here we obtain analogs of Gaussian integrals for finite fields (Theorem 2.10). This calculation is almost trivial, modulo a non-obvious evaluation of the sign. For the last purpose, we need in an examination of Gauss sums.

2.1. Characters of cyclic groups.

Lemma 2.1 *Consider the finite cyclic group $\mathbb{Z}_n$. Let z be its generator Then all the characters of A have form*

$$\Phi_m(kz) = e^{2\pi imk/n}, \qquad m = 0, 1, 2, \ldots, n-1$$

PROOF. Let $\Phi(z) = \mu$. Then $\Phi(kz) = \mu^k$. Since $nz = 0$, we have $\mu^n = 1$ or $\mu = e^{2\pi im/n}$. □

2.2. Additive characters of a finite field. Starting this place until the end of the section denote

$$\boxed{\lambda = \exp\{2\pi i/p\}} \tag{2.1}$$

Consider the functions χ_m on $\mathbb{F}_p$ given by

$$\chi_m(x) = \exp\left\{\frac{2\pi imx}{p}\right\} = \lambda^{mx}, \quad j = 0, 1, \ldots, p-1, \quad x \in \mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$$

These functions are nothing but the characters of the additive group of $\mathbb{F}_p$,

We define the ℓ_2-inner product in the space of functions on $\mathbb{F}_p$,

$$\langle f, g\rangle = \sum_{x\in\mathbb{F}_p} f(x)\overline{g(x)}$$

Lemma 2.2 *The functions $p^{-1/2}\chi_k$ constitute an orthonormal basis in $\ell_2(\mathbb{F}_p)$*

Recall the following lemma.

Lemma 2.3 *Let μ be a root of unity, $\mu^n = 1$, $\mu \neq 1$. Then*

$$1 + \mu + \mu^2 + \cdots + \mu^{n-1} = 0$$

PROOF OF LEMMA 2.3. Multiplying the left-hand side by μ, we obtain the same expression. □

PROOF OF LEMMA 2.2. We must evaluate sums

$$\langle\chi_k, \chi_m\rangle \sum_{x=0}^{p-1} \lambda^{kx}\overline{\lambda}^{mx} = \sum_{k=0}^{p-1} \lambda^{(k-m)x}$$

If $k \neq m$, then after a change of order we come to $\sum_{x=0}^{p-1} \lambda^x = 0$ (because all the powers appearing in our sum are different). □

2.3. The finite Fourier transform. We define the Fourier transform

$$\mathcal{F} : \ell_2(\mathbb{F}_p) \to \ell_2(\mathbb{F}_p)$$

by

$$\mathcal{F}f(y) = \frac{1}{\sqrt{p}} \sum_{x \in \mathbb{F}_p} f(y) \exp\Big\{\frac{2\pi i x y}{p}\Big\} \tag{2.2}$$

We can also say that the Fourier transform is the operator with matrix $\{\lambda^{xy}\}/\sqrt{p}$, where λ is the same as above (2.1),

$$\mathcal{F} = \frac{1}{\sqrt{p}} \begin{pmatrix} 1 & 1 & 1 & \dots & 1 \\ 1 & \lambda & \lambda^2 & \dots & \lambda^{p-1} \\ 1 & \lambda^2 & \lambda^4 & \dots & \lambda^{2(p-1)} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & \lambda^{p-1} & \lambda^{2(p-1)} & \dots & \lambda^{(p-1)^2} \end{pmatrix} \tag{2.3}$$

Theorem 2.4 *a) The operator $\mathcal{F} : \ell_2(\mathbb{F}_p) \to \ell_2(\mathbb{F}_p)$ is unitary.*

b) The inversion formula is

$$f(x) = \frac{1}{\sqrt{p}} \sum_{y \in \mathbb{F}_p} \mathcal{F}f(y) \exp\Big\{-\frac{2\pi i x y}{p}\Big\} \tag{2.4}$$

PROOF. This is completely trivial. The functions $e_m = p^{-1/2}\chi_{-m}$ constitute an ortonormal basis. The statement b) claims

$$f = \sum \langle f, e_m \rangle e_m = v$$

and the statement a) is

$$\langle f, f \rangle = \sum |\langle f, e_m \rangle|^2 \qquad \square$$

Problem 2.1 Show that $\mathcal{F}^2 f(x) = f(-x)$. Hence $\mathcal{F}^4 = 1$.

2.4. Multiplicative characters. Denote

$$\boxed{\mu := \exp\{2\pi i/(p-1)\}}$$

Let ζ be a generator of the group $\mathbb{F}_p^*$. Consider the functions $\Psi_l : \mathbb{F}_p^* \to \mathbb{C}^*$ given by

$$\Psi_l(\zeta^h) = \mu^{hl}$$

These functions are nothing but the multiplicative characters of $\mathbb{F}_p^*$,

$$\Psi_l(uv) = \Psi_l(u)\Psi_l(v)$$

Lemma 2.5 *The system of functions $\Psi_l(x)$, constitutes an orthogonal basis in $\ell_2(\mathbb{F}_p^*)$.*

See Subsection 2.2.

Lemma 2.6

$$\Psi_{(p-1)/2}(x) = \left(\frac{x}{p}\right) \tag{2.5}$$

PROOF. By definition $\mu^{(p-1)/2} = -1$. Hence

$$\Psi_{(p-1)/2}(\mu^j) = \mu^{(p-1)j/2} = (-1)^j$$

But $\eta(\mu^j)$ also is $(-1)^j$. □

Lemma 2.7 $\Psi_k(-1) = (-1)^k$.

PROOF. First, $\Psi_k\big((-1)(-1)\big) = \Psi_k(1) = 1$. Hence $\Psi_k(-1) = \pm 1$. If $\Psi_1(-1) = 1$, then $\Psi_k(-1) = 1$ for all k. But functions Ψ_k form a basis in $\ell_2(\mathbb{F}^*)$, therefore there exists a function Ψ_k having different values at (-1) and 1. This contradiction finishes a proof. □

2.5. Gauss sums. We are going to consider analogs of the integrals

$$\int_0^\infty t^{s-1} e^{-at}\, dt = \Gamma(s) a^{-s} \tag{2.6}$$

Analogs of the factor e^{-zt} are the additive characters of $\mathbb{F}_p$, analogs of the factor t^{s-1} are the multiplicative characters, and the analogs of the integral are $\ell_2(\mathbb{F}_p)$-inner products of additive and multiplicative characters.

Gauss sums are sums of the form

$$\mathfrak{S}_{km} = \mathfrak{S}(\chi_k, \Psi_m) = \sum_{u \in \mathbb{F}_p^*} \chi_k(u) \Psi_m(u)$$

In other words,

$$\mathcal{F}\Psi_m(j) = \mathfrak{S}_{jm}$$

Theorem 2.8 *a) Let $m = 1, \dots, p-2$. Extend each Ψ_m to the whole $\mathbb{F}_p$ by the assumption $\Phi_m(0) = 0$. Then*

$$\mathcal{F}\Psi_m = \Gamma_{\mathbb{F}_p}(m)\, \overline{\Psi_m}$$

where

$$\Gamma_{\mathbb{F}_p}(m) := \frac{1}{\sqrt{p}} \sum_{y \in \mathbb{F}_p{}^*} \chi_1(y) \Psi_m(y)$$

b) The factor $\Gamma_{\mathbb{F}_p}$ satisfies the following properties

$$|\Gamma_{\mathbb{F}_p}(m)| = 1, \tag{2.7}$$

$$\Gamma_{\mathbb{F}_p}(-m) = (-1)^m \overline{\Gamma_{\mathbb{F}_p}(m)} \tag{2.8}$$

PROOF. a) We imitate the substitution $s = at$ to the integral (2.6):

$$\sqrt{p}\mathcal{F}\Psi_m(x) = \sum_{y\neq 0} \chi_1(xy)\Psi_m(y) =$$

$$= \sum_{z\neq 0} \chi_1(z)\Psi_m(x^{-1}z) = \Psi_m(x)^{-1} \sum_{z\neq 0} \chi_1(z)\Psi_m(z)$$

b) Since $\mathcal{F}$ is unitary, we have

$$\|\Psi_k\|_{\ell_2} = \|\mathcal{F}\Psi_k\|_{\ell_2} = |\Gamma_{\mathbb{F}_p}(k)| \cdot \|\Psi_{-k}\|_{\ell_2}$$

and this implies (2.7).

Further,

$$\sqrt{p}\mathcal{F}\Psi_{-k}(x) = \sum_y \chi_1(xy)\Psi_{-k}(y) = \sum_y \chi_1(xy)\overline{\Psi_k(y)} =$$

$$= \sum_y \overline{\overline{\chi_1(xy)}\Psi_k(y)} = \sum_y \overline{\chi_1((-x)y)\Psi_k(y)} = \sqrt{p}\overline{\mathcal{F}\Psi_k(-x)} = (-1)^k\sqrt{p}\mathcal{F}\Psi_k(x)$$

2.6. Fourier transform of the Legendre character.

Theorem 2.9

$$\Gamma_{\mathbb{F}_p}\left(\frac{p-1}{2}\right) = i^{(p-1)^2/4} = \begin{cases} 1 \ \textit{if}\ p = 4k+1 \\ i \ \textit{if}\ p = 4k+3 \end{cases} \tag{2.9}$$

PROOF. First, we determine

$$\Gamma_{\mathbb{F}_p}\left(\frac{p-1}{2}\right) = \sum\nolimits_{y\neq 0} \exp\left\{\frac{2\pi i y}{p}\right\}\left(\frac{y}{p}\right) \tag{2.10}$$

to within a sign. By (2.7), $|\Gamma_{\mathbb{F}_p}((p-1)/2| = 1$.

If $p = 4k+1$, then $\eta(-y) = \eta(y)$. Hence (2.10) is real.

If $p = 4k+3$, then $\eta(-y) = -\eta(y)$. Therefore (2.10) is imaginary.

Thus, in these two cases, our sum is ± 1 or $\pm i$ respectively.

Evaluation of the sign is more complicated. Let us evaluate the determinant of the Fourier transform (2.3) in two ways. A priory $\det\mathcal{F} = \pm i$ or $\pm = 1$, because $\mathcal{F}$ is unitary and $\mathcal{F}^4 = 1$.

Firstly, $\det(\mathcal{F})$ is the Vandermonde determinant

$$\det(\mathcal{F}) = p^{-p/2} \prod_{k>m} (\lambda^k - \lambda^m)$$

Denote $\sigma = \exp\{\pi i/p\}$, hence $\sigma^2 = \lambda$. Then

$$\det\mathcal{F} = p^{-p/2} \prod_{k>m} (\sigma^{2k} - \sigma^{2m}) = p^{-p/2} \prod_{k>m} \sigma^{k+m}(\sigma^{k-m} - \sigma^{m-k}) =$$

$$= p^{-p/2}(2i)^{p(p-1)/2}\sigma^{p(p^2-1)/2} \prod_{k>m} \sin\frac{\pi(k-m)}{p} \tag{2.11}$$

Since $\sigma^{2p} = 1$, we get $\sigma^{p(p^2-1)/2} = 1$. Thus, we come to

$$\det \mathcal{F} = p^{-p/2}(2i)^{p(p-1)/2} \prod_{k>m} \sin \frac{\pi(k-n)}{p} \tag{2.12}$$

Therefore

$$\det \mathcal{F} = i^{p(p-1)/2} \tag{2.13}$$

$$\prod_{k>m} \sin \frac{\pi(k-n)}{p} = p^{p/2} 2^{-p(p-1)/2}$$

The second identity is amusing, however it does not matter for us.

Now let us define another basis. We consider the multiplicative characters $\Psi_1, \Psi_2, \ldots, \Psi_{p-2}$ (here $\Psi_0 = 1$ is omited) extended to $\mathbb{F}_p$ by the assumption $\Psi(0) = 0$. We also consider the function $c(x) := 1$ and the function $\delta_{0,x}$ (the last two functions are not orthogonal).

We use Theorem 2.8 about Gauss sums to write out the matrix of $\mathcal{F}$ in this basis. We obtain a block diagonal matrix having only 2×2 and 1×1 blocks. The list of blocks follows.

1. 2×2-blocks corresponding to vectors Ψ_k, Ψ_{-k}:

$$\begin{pmatrix} 0 & \Gamma_{\mathbb{F}_p}(k) \\ \Gamma_{\mathbb{F}_p}(-k) & 0 \end{pmatrix} \tag{2.14}$$

Here $k = 2, 3, \ldots (p-3)/2$.

2. The block corresponding to $c(x)$ and $\delta_{0,x}$

$$\begin{pmatrix} 0 & p^{-1/2} \\ p^{1/2} & 0 \end{pmatrix}$$

3. The 1×1 block $\Gamma_{\mathbb{F}_p}((p-1)/2)$.

The determinant of (2.14) is

$$-\Gamma_{\mathbb{F}_p}(k)\Gamma_{\mathbb{F}_p}(-k) = -(-1)^k \Gamma_{\mathbb{F}_p}(k)\overline{\Gamma_{\mathbb{F}_p}(k)} = -(-1)^k$$

Multiplying together these quantities, we obtain $(-1)^{[(p-3)/2+(p-5)(p-3)/8]}$.

Thus,

$$\det(\mathcal{F}) = (-1)^{(p-1)(p-3)/8} \cdot (-1)\Gamma_{\mathbb{F}_p}((p-1)/2) \tag{2.15}$$

It remains to compare (2.13) and (2.15). □

2.7. Gaussian quadratic sums.

Theorem 2.10 *Let Q be a nondegenerate symmetric $n \times n$ matrix over $\mathbb{F}_p$. If n is even, then*[2]

$$\xi(Q) := \sum_{x \in \mathbb{F}_p^n} \exp\left\{\frac{2\pi i}{p} x Q x^t\right\} = p^{n/2} \cdot \eta\big((-1)^{n/2} \det Q\big) \tag{2.16}$$

[2] Comparatively the real case, we do not write 1/2 in the exponent. Otherwise, we get an additional factor $\eta(2)^n$ in the right-hand side, $\eta(2) = (-1)^{(p-1)^2/8}$.

If n is odd, then

$$\xi(Q) = \sum_{x\in\mathbb{F}_p^n} \exp\Big\{\frac{2\pi i}{p} xQx^t\Big\} = p^{n/2}\cdot\eta\big((-1)^{(n-1)/2}\det Q\big)\cdot\Gamma_{\mathbb{F}_p}\big((p-1)/2\big) \tag{2.17}$$

PROOF. Since $\Gamma_{\mathbb{F}_p}\big((p-1)/2\big)^2 = \eta(-1)$ the right-hand sides are multiplicative in the following sense

$$\xi(Q_1\oplus Q_2) = \xi(Q_1)\xi(Q_2)$$

The left-hand sides are multiplicative in the same sense.

Since we can reduce a form to a sum of squares, it suffices to verify the identity for $n=1$. Let $r\in\mathbb{F}_p^*$ be a quadratic nonresidue. Denote

$$H_1 := \sum_{x\in\mathbb{F}_p}\exp\Big\{\frac{2\pi i}{p}x^2\Big\},\qquad H_2 := \sum_{x\in\mathbb{F}_p}\exp\Big\{\frac{2\pi i}{p}rx^2\Big\}$$

We have

$$H_1 = 1+2\sum_{y\in(\mathbb{F}_p^*)^2}\exp\Big\{\frac{2\pi i}{p}y\Big\},\qquad H_2 = 1+2\sum_{y\in\mathbb{F}_p^*\setminus(\mathbb{F}_p^*)^2}\exp\Big\{\frac{2\pi i}{p}y\Big\},$$

Hence

$$H_1+H_2 = 2\sum_{y\in\mathbb{F}_p}\exp\Big\{\frac{2\pi i}{p}y\Big\} = 0$$

$$H_1-H_2 = 2\sum_{y\in\mathbb{F}_p^*}\exp\Big\{\frac{2\pi i}{p}y\Big\}\cdot\eta(y) = 2\sqrt{p}\,\Gamma_{\mathbb{F}_p}((p-1)/2)$$

Hence

$$H_1 = \sqrt{p}\,\Gamma_{\mathbb{F}_p}((p-1)/2) = -H_2$$ □

Proposition 2.11 *Let Q be a nondegenerate $n\times n$ symmetric matrix, let $b\in\mathbb{F}_p^n$. Then*

$$\sum_{x\in\mathbb{F}_p^n}\exp\Big\{\frac{2\pi i}{p}(xQx^t+bx^t)\Big\} = \xi(Q)\exp\Big\{-\frac{2\pi i}{p}\cdot\frac{1}{4}bQ^{-1}b^t\Big\}$$

PROOF. We transform the sum to the form

$$\exp\Big\{-\frac{2\pi i}{p}\cdot\frac{1}{4}bQ^{-1}b^t\Big\}\exp\Big\{\frac{2\pi i}{p}(x+b/2)Q(x^t+b^t/2)\Big\}$$

and pass to the variable $y = x+b/2$. □

It is easy to extend these results to degenerate forms. Let B be a quadratic form on a linear space V, denote $W = \ker B$. Let $\widetilde{B}$ be the form induced by B on V/W, let $\widetilde{B}^\circ$ be dual form on the dual space $(V/W)^\circ$. Let ℓ be a linear functional on V. Then

$$\sum_{x\in V} \exp\Bigl\{\frac{2\pi i}{p}(B(x)+\ell(x))\Bigr\} = \begin{cases} p^{\dim W}\xi(\widetilde{B})\exp\Bigl\{-\frac{2\pi i}{p}\cdot\frac{1}{4}\widetilde{B}^\circ(\ell)\Bigr\} & \text{if } \ell = 0 \text{ on } W \\ 0 & \text{otherwise} \end{cases}$$

Indeed, we decompose $W = \ker B \oplus Y$, where Y is a complementary subspace. Now the statement becomes obvious.

9.3 Gaussian operators

This Section is almost independent on the previous two sections.

3.1. Gaussian operators. Let $L \subset \mathbb{F}^m \oplus \mathbb{F}^k$ be a subspace. Let Q be a quadratic form on this subspace. A *Gaussian operator* is an operator

$$B[Q;L] : \ell_2(\mathbb{F}_p^k) \to \ell_2(\mathbb{F}_p^m)$$

given by the formula

$$B[Q;L]f(x) = \lambda \sum_{y\in\mathbb{F}_p^k:\,(x,y)\in L} \exp\Bigl\{-\frac{\pi i}{p}Q(x\oplus y)\Bigr\}\, f(y)$$

Where $\lambda \in \mathbb{C}^*$ is a nonzero constant.

Theorem 3.1 *a) A product of Gaussian operators is a Gaussian operator.*

b) The category of Gaussian operators defined to within scalars is equivalent to the category of Lagrangian linear relations over $\mathbb{F}_p$.

A proof occupies the rest of this section.

3.2. Heisenberg group over $\mathbb{F}_p$. Let $\mathcal{V}_{2n}$ be a $2n$-dimensional space over $\mathbb{F}_p$ endowed with a nondegenerate skew-symmetric bilinear form $S(\cdot,\cdot)$. We define the product on $\mathcal{V}_{2n} \oplus \mathbb{F}_p$ by

$$(u,x)\circ(v,y) = \bigl(u+v, x+y+\frac{1}{2}S(u,v)\bigr) \tag{3.1}$$

Problem 3.1 We obtain a group.

This group is called the *Heisenberg group* $\mathrm{Heis}_n(\mathbb{F}_p)$ over field $\mathbb{F}_p$.

The subgroup $Z := 0\oplus\mathbb{F}_p$ is the center of Heis_n. The quotient group Heis_n/Z is the additive group of $\mathcal{V}_{2n}$.

3.3. The standard representation of Heis_n. Denote

$$\mathcal{V}_{2n} := \mathcal{V}_n^+ \oplus \mathcal{V}_n^- :\simeq \mathbb{F}_p^n \oplus \mathbb{F}_p^n$$

equipped with the form $\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$.

For an element $(v^+ \oplus v^-, h) \in \mathrm{Heis}_n(\mathbb{F}_p)$ consider the operator $T_\alpha(v^+ \oplus v^-, h)$ in $\ell_2(\mathbb{F}_p^n)$ given by

$$T(v^+ \oplus v^-, h) = f(x + v^+) \exp\Big\{\frac{2\pi i}{p} v^- x^t\Big\} \cdot \exp\Big\{\frac{2\pi i}{p}\big[h + \frac{1}{2} v_+ (v_-)^t\big]\Big\}$$

A straightforward calculation shows that such operators form the Heisenberg group.

3.4. Gaussian vectors and their stabilizers. Let M be a subspace in $\mathbb{F}_p^n$, let R be a quadratic form on M. Let $\lambda \in \mathbb{C}$. A *Gaussian vector* in $\ell_2(\mathbb{F}_p^n)$ is a function of the form

$$b[R; M] = \begin{cases} \lambda \cdot \exp\{-\frac{\pi i}{p} R(x)\} & \text{if } x \in M \\ 0 & \text{otherwise} \end{cases}$$

For a Gaussian vector $b[R, M]$ is a Gaussian vector denote by $W = W[R, M]$ the subspace in $\mathcal{V}_{2n}$ consisting of v such that

$$T(v; 0) b[R; M] = b[R; M] \tag{3.2}$$

Theorem 3.2 *a) W is Lagrangian subspace in $\mathcal{V}_{2n}$*

b) The vector $b[R; M]$ is a unique vector f satisfying

$$T(v; 0) f = f \qquad \text{for all } v \in W$$

c) We get a bijection

$$\left\{\begin{matrix} \text{Lagrangian Grassmannian} \\ \text{in } \mathcal{V}_{2m} \end{matrix}\right\} \leftrightarrow \left\{\begin{matrix} \text{The set of Gaussian vectors} \\ \text{defined to within a scalar} \end{matrix}\right\}$$

PROOF. First, let $M = \mathbb{F}_p^n$. Denote $v = v_+ \oplus v_-$. Then

$$\begin{aligned} T(v_+ \oplus v_-, 0) \exp\Big\{-\frac{\pi i}{p} x R x^t\Big\} &= \\ = \exp\Big\{-\frac{\pi i}{p}(x + v_+) R (x + v_+)^t\Big\} \cdot \exp\Big\{\frac{2\pi i}{p} x v_-\Big\} \cdot \exp\Big\{\frac{\pi i}{p} v_+ v_-^t\Big\} &= \\ = \exp\Big\{-\frac{\pi i}{p} x R x^t\Big\} \cdot \exp\Big\{\frac{2\pi i}{p}\big[x v_-^t - x R v_+^t\big]\Big\}& \end{aligned}$$

The condition (3.2) is satisfied iff

$$v_- = v_+ R$$

By Theorem 3.1.4, this constrain determines a Lagrangian subspace. Obviously, this subspace 'remembers' a Gaussian vector.

Next, let M be a proper subspace. Without loss of generality, we can assume that M is a coordinate subspace $v_1 = \cdots = v_{k-m} = 0$ in $\mathbb{F}_p^n$. Our Gaussian vector is fixed under multiplications by functions $\exp\{\sum_{j>k} v_j^- x_j\}$.

Decompose $\mathcal{V}_{2n} = \mathcal{V}_{2(n-m)} \oplus \mathcal{V}_{2m}$. Evidently, the subspace W consists of vectors

$$v_+ \oplus v_- \oplus w_+ \oplus w_-, \qquad \text{where } v_- = v_+ R \text{ and } w_+ = 0$$

Thus W is a direct sum of two Lagrangian subspaces, hence it is Lagrangian.

To prove b), we repeat the arguments of Theorem 1.6.1.b. □

3.5. Gaussian operators and Lagrangian linear relations. Equip $\mathcal{V}_{2k} \oplus \mathcal{V}_{2m}$ with the *difference* of skew-symmetric bilinear form as above, see Subsection 1.8.1.

Theorem 3.3 *a) Let $B[Q;L]$ be a Gaussian operator $\ell_2(\mathbb{F}_k) \to \ell_2(\mathbb{F}_m)$. Consider the set $W = W[Q;L] \subset \mathcal{V}_{2k} \oplus \mathcal{V}_{2m}$ consisting of vectors $u \oplus v$ satisfying*

$$T(v;0)B[Q;L] = B[Q;L]T(u;0) \tag{3.3}$$

Then W is a Lagrangian subspace in $\mathcal{V}_{2k} \oplus \mathcal{V}_{2m}$.

b) The operator $B[Q;L]$ is a unique to within a scalar operator $A : \ell_2(\mathbb{F}_p^k) \to \ell_2(\mathbb{F}_p^m)$ satisfying

$$T(v;0)A = AT(u;0) \qquad \text{for all } u \oplus v \in W \tag{3.4}$$

c) The map $B[Q;L] \mapsto W$ is a bijection

$$\begin{Bmatrix} \text{The set of Gaussian operators} \\ \text{defined to within scalars} \end{Bmatrix} \leftrightarrow \begin{Bmatrix} \text{Lagrangian Grassmannian} \\ \text{in } \mathcal{V}_{2k} \oplus \mathcal{V}_{2m} \end{Bmatrix}$$

d) Let

$$B[Q;L] : \ell_2(\mathbb{F}_p^k) \to \ell_2(\mathbb{F}_p^m) \qquad , B[Q';L'] : \ell_2(\mathbb{F}_p^m) \to \ell_2(\mathbb{F}_p^n)$$

be Gaussian operators. Then the product $B[Q';L')B[Q;L]$ is a nonzero operator and it corresponds to the product $W[Q';L']W[Q;L]$ of linear relations

PROOF. A matrix of an operator $A : \mathbb{F}_p^k \to \mathbb{F}_p^m$ is a function on $\mathbb{F}_p^k \oplus \mathbb{F}_p^m$. The equation (3.4) is nothing but the equation (3.2) Gaussian vector; only several signs are changed. Hence the statements a)-c) are nothing but a rephrasing of Theorem 3.2.

To prove c), we repeat the arguments of Subsection 1.9.4. Let $u \oplus v \in W[Q;L)$, $v \oplus y \in W[Q';L']$. Then

$$B[Q';L']B[Q;L]T(u;0) = B[Q';L']T(v;0)B[Q;L] = T(y;0)B[Q';L']B[Q;L]$$

Thus, $B[Q';L']B[Q;L]$ satisfies to the relations (3.4) with $W = W[Q';Y']W[Q;Y]$. A reference to the statement b) almost proves d).

It remains to show that a product of nonzero Gaussian operators is nonzero.

Observation 3.4 *For any quadratic form Q on $\mathbb{F}_p^n$,*

$$\sum_{x\in\mathbb{F}_p^n} \exp\Big\{\frac{\pi i}{p} Q(x)\Big\} \neq 0$$

Indeed, we know explicit formulae. □

Continue the proof of the theorem. Let $b_1 \in \mathbb{F}_p^k$, $b_2 \in \mathbb{F}_p^m$ be Gaussian vectors, B be a Gaussian operator. The expression

$$\langle B \cdot b_1, b_2\rangle_{\ell_2(\mathbb{F}_p^m)}$$

is a Gaussian quadratic sum and hence it is non-zero. Hence $Bb_1 \neq 0$. However, this vector is Gaussian.

Observation 3.5 *A Gaussian operator takes Gaussian vectors to Gaussian vectors.*

Proof. As in Subsection 1.3.11, we regard Gaussian vectors as Gaussian operators $0 \to \mathbb{F}_p^k$. However, the statement about operators is already proved.□

Hence a product of Gaussian operators takes a Gaussian vector to a *nonzero* Gaussian vector. □

Problem 3.2 Construct the Weil representation of $\mathrm{Sp}(2n, \mathbb{F}_p)$ as it was done in Theorem 1.2.7

3.6. Digression. Suprunenko gradations of semisimple Lie algebras.

Problem 3.3 a) Consider the action of $\mathrm{Heis}_n(\mathbb{F}_p)$ on the Lie algebra $\mathfrak{g} := \mathfrak{sl}(p^n, \mathbb{C})$ by automorphisms

$$X \mapsto T(v;h)^{-1} X T(v;h)$$

Since $T(0;h)$ are scalar operators, we obtain an action of the Abelian group $V_{2n} \simeq \mathbb{F}_p^{2n}$. Show that for each nontrivial character $\chi : \mathbb{F}_p^{2n} \to \mathbb{C}^*$, the eigenspace $\mathfrak{g}_\chi$:

$$X \in \mathfrak{g}_\chi \text{ if } T(v;0)^{-1} X T(v;0) = \chi(v) X$$

is one-dimensional. For the trivial character $\chi(v) = 1$, this subspace is trivial. Show that

$$[\mathfrak{g}_\chi, \mathfrak{g}_\varphi] = \begin{cases} \mathfrak{g}_{\chi\varphi} & \text{if } \chi\varphi \neq 1 \\ 0 & \text{otherwise} \end{cases}$$

Thus, we get a gradation of the Lie algebra $\mathfrak{sl}(p^n, \mathbb{C})$.

b) Describe this gradation explicitly for $n = 1$.

9.4 Fast Fourier transform

Numerical evaluation of the Fourier transform rather often appears in applied problems. Here we discuss, fast ways of such calculations.

Let N be a large (generally not prime) positive integer. By $\mathbb{Z}_N = \mathbb{Z}/\mathbb{Z}_N$ we denote the cyclic group of order N. The Fourier transform on this group is defined in the usual way,

$$\mathcal{F}_N f(x) = \sum_{k=0}^{N-1} \exp\Big\{\frac{2\pi i}{N} xy\Big\} f(y)$$

At first glance this calculation requires N^2 multiplications[3]. In fact, tricks discussed below allow to evaluate $\mathcal{F}_N f$ using

$$\leqslant \mathrm{const} \cdot N \log_2 N \tag{4.1}$$

operations (in fact, this constant is $\leqslant 8$). This phenomenon drastically expands possibilities of numerical calculations of Fourier transforms.

In this section, we discuss several approaches to this problem. Denote

$$\lambda := \exp\Big\{\frac{2\pi i}{N}\Big\}, \qquad a_j := f(j), \qquad b_m := \mathcal{F} f(m)$$

4.1. The Cooley–Tukey trick. Let $N = 2^n$. We must evaluate all the numbers

$$\begin{aligned} b_m &= a_0 + \lambda^m a_1 + \lambda^{2m} a_2 + \lambda^{3m} a_3 + \dots = \\ &= \Big[a_0 + \lambda^{2m} a_2 + \lambda^{4m} a_4 + \dots\Big] + \lambda^m \Big[a_1 + \lambda^{2m} a_3 + \lambda^{4m} a_5 + \dots\Big] \end{aligned}$$

Next, λ^2 is a primitive root of unity of degree $N/2$. Therefore the expressions in the square brackets are Fourier transforms of vectors $\{a_{2j}\}$ and $\{a_{2j+1}\}$ on the group $\mathbb{Z}_{N/2}$.

Now we must evaluate two Fourier transforms on the group $\mathbb{Z}_{N/2}$ instead of one Fourier transform on $\mathbb{Z}_N$. This require $(N/2)^2 + (N/2)^2$ multiplications instead of N^2. Thus, the number of required multiplications is reduced by two times.

But we can evaluate the Fourier transforms on $\mathbb{Z}_{N/2}$ in the same way. Etc.

This trick allows to evaluate the Fourier transform on $\mathbb{Z}_N = \mathbb{Z}_{2^n}$ using

$$\leqslant \frac{3}{2} N \log_2 N$$

multiplications.

[3] Also it requires N^2 additions, but an addition is a 'short' computer operation comparatively with a multiplication. Also an evaluation of Fourier transforms requires calculations of N exponents (which can be tabulated) and (may be) some auxiliary 'short' operations. The main contribution to the total computer time is given by multiplications.

4.2. A variation of the same trick. Let $N = qr$ be a composite number. First, assume that q and r are relatively prime. Then $\mathbb{Z}_N \simeq \mathbb{Z}_q \times \mathbb{Z}_r$, and we can decompose the Fourier transform

$$\mathcal{F}_N = \mathcal{F}_q \circ \mathcal{F}_r$$

To evaluate $\mathcal{F}_N$, we must evaluate q Fourier transforms on sets $j \times \mathbb{Z}_r$ and r Fourier transforms on the sets $\mathbb{Z}_q \times k$.[4]

Now let $N = qr$, where q and r are arbitrary. We write

$$b_m = \sum_{j=0}^{q-1} \lambda^{mj} \Big[a_j + \lambda^{mq} a_{j+q} + \lambda^{2mq} a_{j+2q} + \dots \Big]$$

Next, we represent $m = lr + k$, where $0 \leqslant k < r$. Then

$$b_m = \sum_{j=0}^{q-1} (\lambda^r)^{lj} \cdot \lambda^{kj} \Big[a_j + \lambda^{mq} a_{j+q} + \lambda^{2mq} a_{j+2q} + \dots \Big]$$

Note that λ^q is a primitive root of unity of degree r and λ^r is a primitive root of degree q. In square brackets, we have $\mathcal{F}_r$-transforms of q vectors.

After this, the evaluation of $(b_k, b_{r+k}, b_{2r+k}, \dots)$ is nothing but an evaluation of a certain $\mathcal{F}_q$-transform. Thus, we must also evaluate r items of $\mathcal{F}_q$ transforms.

Remark. Actually, this calculation is completely parallel to calculation (8.2.4). In the latter case, we evaluate the Zak transform and reduce the Fourier transform to the Zak transform.

4.3. Fast convolution. The convolution on the group $\mathbb{Z}_N$ is defined in the usual way,

$$f * g(k) = \sum_{j \in \mathbb{Z}_N} f(j) g(k - j)$$

As usual, the Fourier transform takes convolutions to products.

Hence, having a fast way to evaluate the Fourier transform on $\mathbb{Z}_N$, we have a fast way to evaluate convolutions: we simply evaluate $\mathcal{F}_N^{-1}(\mathcal{F}_N f \cdot \mathcal{F}_N g)$.

Remark. If the operation in the group G is called a multiplication, then

$$f * g(x) = \sum_y f(x/y) g(y) = \sum_{xy} f(xy) g(y^{-1})$$

4.4. Prime N. Now let $N = p$ be a prime. We must evaluate the vectors

$$c_m := \sum_{j=0}^{p-1} \lambda^{mj} a_j$$

[4] also, we must spend some time for reordering of the set $\mathbb{Z}_N$.

where $m = 0, 1, \ldots, p-1$ It suffices to find a fast way to evaluate the numbers

$$h_m := \sum_{j=1}^{p-1} \lambda^{mj} a_j \qquad \text{where } m \neq 0$$

Now the summation is taken over the multiplicative group $\mathbb{F}_p^* \simeq \mathbb{Z}_{p-1}$. The function $h(-m)$ is nothing but a convolution of the function $g(k) := a_k$ and the function $f(l) := \lambda^{-l}$ on the multiplicative group $\mathbb{F}_p^*$.

It remains to note, that the number $p-1$ is composite and we can repeat the Cooley–Tukey trick[5].

4.5. Another way. For definiteness, assume, that N is even (otherwise, the considerations given below must be slightly modified).

$$b_m = \sum_{j=0}^{N-1} \lambda^{mj} a_j = \lambda^{m^2/2} \sum_{j=0}^{N-1} \lambda^{-(m-j)^2/2} \lambda^{j^2/2} a_j$$

here we assume $\lambda^{1/2} := \exp\{\pi i/N\}$. We observe that the vector

$$w_m := \lambda^{-m^2/2} b_m$$

is a convolution of the vectors

$$u_j := \lambda^{j^2/2} a_j, \qquad \text{and} \qquad v_k := \lambda^{-k^2/2}$$

Since N is even,

$$v_{k+N} = \exp\Big\{\frac{\pi i}{N} \cdot (k^2 + 2kN + N^2)\Big\} = \exp\Big\{\frac{\pi i}{N} \cdot k^2\Big\} = v_k$$

therefore v_k and u_k are well-defined functions on $\mathbb{Z}_N$.

Let $M \geqslant 2N$. We wish to evaluate the same convolution as a convolution on the group $\mathbb{Z}_M$. For this goal, consider the functions on $\mathbb{Z}_M$ given by

$$U_j := \begin{cases} u_j & \text{if } 0 \leqslant j < N \\ 0 & \text{otherwise} \end{cases}, \qquad V_k := \begin{cases} v_k & \text{if } 0 \leqslant j < N \\ v_{-k} & \text{if } -N < j \leqslant 0 \\ 0 & \text{otherwise} \end{cases}$$

Let $W := V * U$ be their convolution. Evidently,

$$W_j = w_j, \qquad \text{for } 0 \leqslant j < N$$

Thus, we can evaluate the Fourier transform on $\mathbb{Z}_N$ as a convolution on the group $\mathbb{Z}_M$ with $M \geqslant 2N$.

Now we can choose M in the form $M = 2^n$. If we fight for an improvement of the constant in (4.1) we can choose an appropriate number 2^n, $3 \cdot 2^n$, $3^2 \cdot 2^n$, $3^3 \cdot 2^n$, $5 \cdot 2^n$ and apply the trick given above.

[5]However, it is also necessary to find a generator of $\mathbb{F}_p^*$ and identify its power with residues modulo p.

9.5 Bibliographic remarks

5.1. Gauss sums were investigated by K.F.Gauss himself, this topic is exposed in infinite numbers of text-books, for instance [20], [162], [93]; our presentation is far to be complete.

5.2. Gaussian operators. Weil representation of $\mathrm{Sp}(2n, \mathbb{F}_p)$ was introduced by A.Weil. Theorem 3.3 was announced in [113].

5.3. Exotic gradations of semisimple Lie algebras. As far as I know they were introduced by D.A.Suprunenko in 1960-s. For further extensions, see [4], [87].

5.4. Fast Fourier transform. See, for, instance [32] and further references in this book. The trick of Subsection 4.1 usually is attributed to J.W.Cooley and J.W.Tukey, but apparently it was known in time of hand computations. In literature, I met also an attribution of this trick to Gauss, I myself did not seen this work. The construction 4.4 is attributed to C.M.Rader, and 4.5 to L.I.Bluestein.