Linear Algebra

Lecture 4: Quadratic Forms over Finite Fields

Nikolay V. Bogachev

Moscow Institute of Physics and Technology,
Department of Discrete Mathematics,
Laboratory of Advanced Combinatorics and Network Applicationss

Quadratic Residues

Let $\mathrm{k} = \mathbb{Z}_p$ with a prime $p \neq 2$. Then $\mathbb{Z}_p^*$ is a cyclic group and $(\mathbb{Z}_p^*)^2 = \{a^2 \mid a \in \mathbb{Z}_p^*\}$ is its subgroup of index 2.

Elements of $(\mathbb{Z}_p^*)^2$ are called quadratic residues, and elements from $\mathbb{Z}_p^* \setminus (\mathbb{Z}_p^*)^2$ are quadratic nonresidues.

Quadratic Equation over $\mathbb{Z}_p$

For every non-degenerate quadratic form q over $\mathbb{Z}_p, (p \neq 2)$, there $\exists$ a solution of $q(x) = 1$.

Proof: $n = 2$: $q(x) = a_1x_1^2 + a_2x_2^2$, $a_1, a_2 \neq 0$. Then we solve $a_1x_1^2 = 1 - a_2x_2^2$. The left-hand side assumes $\frac{p+1}{2}$ distinct values and the right-hand side as well. Since $\frac{p+1}{2} + \frac{p+1}{2} > p$, then there exists a common value for both sides. ∎

Normal Forms over $\mathbb{Z}_p$

Every non-degenerate quadratic form q over $\mathbb{Z}_p$, $(p \neq 2)$, can be reduced to $x_1^2 + \ldots + x_n^2$ or $x_1^2 + \ldots + x_{n-1}^2 + \varepsilon x_n^2$, where ε is a quadratic non-residue.

Proof: For $n \geq 2$ $\exists e_1$: $q(e_1) = 1$. Then we have $V = \langle e_1 \rangle \oplus \langle e_1 \rangle^{\perp}$. And we can continue the procedure. Finally, it remains $q(e_n)$.

Normal Forms over $\mathbb{Z}_p$

Proof continuation: That is,
$Q' = \mathrm{diag}(1, \ldots, 1, q(e_n)) = C^T QC$ and
$\det Q' = (\det C)^2 \cdot \det Q$.

It implies that $q(e_n)$ will be a quadratic residue or nonresidue depending on $\det Q$. $\blacksquare$

Symplectic Basis

Let α be a skew-symmetric over any k. Then there $\exists$ a (symplectic) basis s.t. the matrix of α is the direct sum of blocks

$$U = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$$

Proof: There $\exists e_1, e_2$ such that $\alpha(e_1, e_2) = -\alpha(e_2, e_1) = 1$. That is, $\mathrm{Mat}(\alpha\mid_{\langle e_1, e_2\rangle}) = U$. It remains to use that $V = \langle e_1, e_2\rangle \oplus \langle e_1, e_2\rangle^{\perp}$. ■