Eight's week notes

J.K.

These notes briefly explain the material I planned to cover in the eight week. It is selected from [1, 3, 4]. Other material relevant for algebraic proof systems is listed in the syllabus in Section 4. In particular, I do not comment on related material here (this can be found also in the cited papers, all available).

1 Definitions and (a generalisation of) Ajtai's theorem

The variables $x_{i,j}$ in PHP_n are indexed by ordered pairs and hence monomials by ordered tuples. In $Count^n_m$ the variables x_e are indexed by unordered m-tuples and hence monomials formed from those are indexed by ordered tuples of unordered m-tuples. This leads to the following definition.

A prime p is fixed for the whole note.

Definition 1.1 *Let M be any set containing a fixed set of constants C.*

1. *$Index(M,k)$ is the set of k-tuples $i = (i_1, \dots, i_k)$ of finite subsets of M such that $|i_j| \leq k$, all $j \leq k$. The elements of $Index(M,k)$ are called k-ary indices over M. The support of i is the set $supp(i) := \bigcup_j i_j$.*
2. *$M^{(k)}$ is the $\mathbf{F}_p$-vector space generated by $Index(M,k)$.*

From now on we always assume $M \supseteq C$.

Definition 1.2 *Let $i \in Index(M,r)$.*

The type of i, denoted $\mathbf{tp}_C(i)$, is the isomorphism type of the finite structure

$$\langle C \cup supp(i); \{c\}_{c \in C}, i_1, \dots, i_r \rangle$$

with the universe $C \cup supp(i)$.

The type of a pair (i,j), $i \in Index(M,\ell)$ and $j \in Index(M,k)$ is the type of the $k+\ell$-index i followed by j.

$\Omega_{\ell,k}$ is the set of all types of such pairs (i,j).

$\mathbf{Sym}(M)$ is the group of permutations of M fixing point-wise the set C.

The vector space $M^{(k)}$ is also closed under the action of $\mathbf{Sym}(M)$ and so it is a group-algebra module, an $\mathbf{F}_p[\mathbf{Sym}(M)]$-module. Given its submodule W we shall say that a set $G \subseteq M^{(k)}$ *generates* W iff it generates W as an $\mathbf{F}_p[\mathbf{Sym}(M)]$-module, and that it *generates* W *as a vector space* iff W is the $\mathbf{F}_p$-linear span of G.

Definition 1.3 *A uniform (k,ℓ)-family of vector spaces is a map*

$$V : \Omega_{\ell,k} \to \mathbf{F}_p$$

The family is indexed by M: $\{V^M\}_M$.

Given M, the space V^M has vectors V_i^M for $i \in Index(M,\ell)$. The j-th coordinate of V_i^M, $j \in Index(M,k)$, is:

$$V_{i,j}^M := V(\mathbf{tp}_C((i,j))) \in \mathbf{F}_p$$

So

$$V_i^M = \sum_j V_{i,j}^M j$$

Note that any V^M in a uniform family is, in fact, an $\mathbf{F}_p[\mathbf{Sym}(M)]$-submodule of $M^{(k)}$.

Theorem 1.4 ([1, 3]) *Given $k \geq 1$ there are $\ell \geq 1$ and $c \geq 1$, and uniform (k,ℓ)-systems $H_1, \ldots, H_c$ such that the following holds.*

Let M be arbitrary and let $W \subseteq M^{(k)}$ be arbitrary $\mathbf{F}_p[\mathbf{Sym}(M)]$-submodule. Then one of H_s^M, $s \leq c$, generates W as a vector space.

Remark: This is based on constructions in characteristic-free representation theory of symmetric groups by James [2].

2 Uniform linear systems

We apply Section 1 to families of polynomials.

Definition 2.1

$Var(M,k)$ is the set of variables indexed by elements of $Index(M,k)$ different from $\overline{\emptyset} = (\emptyset, \ldots, \emptyset)$. (The index $\overline{\emptyset}$ will represent 1 in monomials.)

$Mon(M,k,d)$ is the set of all monomials formed from $Var(M,k)$ and of degree at most d. Monomials from $Mon(M,k,d)$ are identified with indices from $Index(M,kd)$, utilising the index $\overline{\emptyset}$ for monomials of degree $\ell \leq d$. In particular, monomial $x_{i^1}x_{i^2}\ldots x_{i^\ell}$, $i^t = (i_1^t, \ldots, i_k^t)$, is identified with the kd-ary index $(i_1^1, \ldots, i_k^1, \ldots, i_1^\ell, \ldots, i_k^\ell, \emptyset, \ldots, \emptyset)$.

A polynomial is a function from some $Mon(M, k, d)$ to $\mathbf{F}_p$, and $Poly(M, k, d)$ is the set of polynomials of degree at most d with variables from $Var(M, k)$.

Note that $Poly(M, k, d)$ is a submodule of $M^{(kd)}$. We say that a family of polynomial systems is *a uniform family* if the corresponding family of submoduli are uniform (kd, ℓ)-family.

Example 2.2 *Fix a parameter $N \geq 1$ (identified with $\{0, 1, \dots, N-1\}$). The variables of the system $\neg PHP^N$ are x_{ij}, where $i \in N$ and $j \in N \setminus \{0\}$. $C := \{0\}$. The system consists of the following polynomials:*

1. $Q_{ij} := x_{ij}^2 - x_{ij}$, *all* i, j.
2. $Q_{i_1, i_2, j} := x_{i_1 j} x_{i_2 j}$, *all* $i_1 \neq i_2$, j.
3. $Q_i := 1 - \sum_j x_{ij}$, *all* i.

We identify a polynomial system $\{F_i\}_i$ with the system of equations $\{F_i = 0\}_i$.

The system is unsolvable for all N: by the first equations each x_{ij} is either 0 or 1, by the remaining equations the set $\{(i, j) \mid x_{ij} = 1\}$ is a graph of an injective mapping from N into $N \setminus \{0\}$, violating the pigeonhole principle (hence the name $\neg PHP^N$).

Example 2.3 *Let $N \geq m \geq 2$. The variables of the system $\neg Count_m^N$ are x_e, where e ranges over $[N]^m$. $C := \emptyset$. The system consists of the following polynomials:*

1. $Q_e \ := \ x_e^2 - x_e$, *for each* e.
2. $Q_{e,f} \ := \ x_e \cdot x_f$, *for every* e, f *such that* $e \cap f \neq \emptyset$ *but* $e \neq f$.
3. $Q_i \ := \ 1 - \sum_{e:\ i \in e} x_e$, *for each* $i \in N$.

Assume that $x_e \ := \ a_e$ is a solution of the system $\neg Count_m^N$ in some integral domain. Then by equations $Q_e = 0$ all a_e are 0 or 1, and by the remaining equations the set

$$\{e \in [N]^m \mid a_e = 1\}$$

is a partition of N into m-element sets. Thus the system has a solution iff m divides N.

Theorem 2.4 ([1]) *Given $k, \ell \geq 1$ there is $\nu \geq 1$ such that the following holds.*

Assume that a family F_i^M, $i \in Index(M, \ell)$, is a uniform family of linear polynomials with variables from $Var(M, k)$ (i.e., it is a (k, ℓ)-family).

Then there exists $Q \subseteq \{0, \dots, p^\nu - 1\}$ such that for every sufficiently large M the system

$$\{F_i^M = 0\}_{i \in Index(M, \ell)}$$

is solvable in $\mathbf{F}_p$ iff $|M| \equiv r \pmod{p^\nu}$ for some $r \in Q$.

Remark: In [4] this is extended to infinite structures M that are equipped with an Euler characteristic χ with values in $\mathbf{Z}/(p^\nu)$.

3 Applications to Nullstellensatz system

It is easy to see that, given a polynomial system F^M (F a uniform family of polynomials indexed by ℓ-indices with variables indexed by k-indices) and a polynomial g^M in the same variables there is a system of linear equations whose solutions correspond to NS-proofs of degree $\leq t$ of g^M from F^M. Call it $NS(t, F, g)^M$. In particular, let $u_{i,j}$ be variables, i ranging over ℓ-indices and j ranging over monomials of degree at most t (i.e., particular tk-indices). Variable $u_{i,j}$ is intended to represent the coefficient (from $\mathbf{F}_p$) of the monomial j in G_i, if $\sum_i G_i F_i = g$ is the alleged NS-proof. Then such G_i of degree at most t exists iff

$$\sum_i \sum_{j_1, j_2 : j_1 \cup j_2 = j} u_{i,j_1} F_{i,j_2} = g_j$$

for all j (we put $g_j := 0$ for monomials j not occurring in g).

The following is easy.

Lemma 3.1 *If F is a uniform family of polynomials indexed by ℓ-indices with variables indexed by k-indices, and g be a uniform polynomial (i.e., a family consisting of one polynomial) with the same variables, then for any fixed t the systems $NS(t, F, g)^M$ is a uniform linear system.*

Degree lower bounds for NS:

Take $F := \neg Count_m$, m not divisible by p. For N' divisible by m, the system $\neg Count_m^{N'} = 0$ has a solution so $NS(t, F, 1)^{N'}$ is unsolvable for any t. But for any N there is an arbitrarily large $N' \equiv N \pmod{p^\nu}$ and $N' \equiv 0 \pmod{m}$. Hence $NS^N(t, F, 1)$ is unsolvable for any N large enough (by Theorem 2.4), i.e. $\neg Count_m^N$ has no bounded degree Nullstellensatz refutations (proofs of 1).

Remark: $\neg PHP^N$ is unsolvable in finite structures. But the generalisation from [4] of Theorem 2.4 to infinite (Euler) structures allows the same argument for Nullstellensatz refutations of $\neg PHP^N$ as well, as a map violating PHP is definable in $\mathbf{R}$, an Euler structure.

4 Applications to polynomial calculus

It is not obvious at all that the space of polynomials from $Poly(M, k, t)$ having a degree $\leq t$ PC-proof from some F^M has description by a uniform linear system. In fact, one cannot use just one such system as in the case of NS.

For the rest of the section let F be a fixed uniform family of degree at most d polynomials with variables indexed by k-ary indices.

Definition 4.1 *For $t \geq d$, $PC_t(M,F)$ is the vector space over $\mathbf{F}_p$ consisting of polynomials from $Poly(M,k,t)$ that have a PC-proof from F^M of degree at most t.*

Lemma 4.2 ([3, L.3.5]) *There are finitely many uniform families H_r of polynomials of degree at most t with variables indexed by k-ary indices, for $r = 0, 1, \ldots, p^\nu - 1$ for some $\nu \geq 1$ depending only on k and t, such that the following holds.*

For every finite M, if $|M| \equiv r$ (mod p^ν) then the system H_r^M generates as a vector space the space $PC_t(M,F)$.

Corollary 4.3 *Given F, g as in Lemma 3.1 there is $\nu \geq 1$ and $Q \subseteq \{0, \ldots, p^\nu - 1\}$ such that g^M has a degree $\leq t$ PC-proof from F^M iff $|M| \equiv r$ (mod p^ν), for some $r \in Q$.*

The ν here is the maximum of the ν's occurring in Theorem 2.4 and Lemma 4.2.

Degree lower bounds for PC:

Take $\neg Count_m$: an identical argument as in the case of NS works.

References

[1] Ajtai, M. (1994) Symmetric systems of linear equations modulo p, a preprint. Available as a report number TR94-015 of the *Electronic Colloquium on Computational Complexity*, http://www.eccc.uni-trier.de/pub/eccc

[2] James, G. D. (1978) *The representation theory of the symmetric groups*, LN in Mathematics, **Vol. 682**,

[3] Krajíček, J. (1997) On the degree of ideal membership proofs from uniform families of polynomials over a finite field, submitted.

[4] Krajíček, J. (1997) Uniform families of polynomial equations over a finite field and structures admitting an Euler characteristic of definable sets, preprint.