GROUP ALGEBRA and the STRUCTURE of PRODUCT SET

Vilnius Conference in Combinatorics and Number Theory

Fedor Petrov

July 17, 2017

Progressions

Progressions

G is a group,

Progressions

G is a group,nontrivial progression in G: $ac = b^2$, a, b, c not all equal

Progressions

G is a group,nontrivial progression in G: $ac = b^2$, a, b, c not all equal
(warning: $ba^{-1} = cb^{-1}$ is a different condition)

Progressions

G is a group,nontrivial progression in G: $ac = b^2$, a, b, c not all equal
(warning: $ba^{-1} = cb^{-1}$ is a different condition)
Maximal size X of a progression-free set in a given finite group G?

Progressions

G is a group,nontrivial progression in G: $ac = b^2$, a, b, c not all equal
(warning: $ba^{-1} = cb^{-1}$ is a different condition)
Maximal size X of a progression-free set in a given finite group G?
$G = C_n$ (cyclic group of order n): K. F. Roth 1953 — $X = o(n)$,

Progressions

G is a group,nontrivial progression in G: $ac = b^2$, a, b, c not all equal
(warning: $ba^{-1} = cb^{-1}$ is a different condition)
Maximal size X of a progression-free set in a given finite group G?
$G = C_n$ (cyclic group of order n): K. F. Roth 1953 — $X = o(n)$,

(K. O'Bryant 2011) $n2^{-\sqrt{8\log_2 n}} \leqslant X \leqslant C\dfrac{(\log\log n)^4}{\log n}n$ (T. Bloom 2016

Progressions

G is a group,nontrivial progression in G: $ac = b^2$, a, b, c not all equal
(warning: $ba^{-1} = cb^{-1}$ is a different condition)
Maximal size X of a progression-free set in a given finite group G?
$G = C_n$ (cyclic group of order n): K. F. Roth 1953 — $X = o(n)$,

(K. O'Bryant 2011) $n2^{-\sqrt{8\log_2 n}} \leqslant X \leqslant C\dfrac{(\log\log n)^4}{\log n}n$ (T. Bloom 2016

$G = C_p^n$: $X = o(|G|^{1-\delta})$,

Progressions

G is a group,nontrivial progression in G: $ac = b^2$, a, b, c not all equal
(warning: $ba^{-1} = cb^{-1}$ is a different condition)
Maximal size X of a progression-free set in a given finite group G?
$G = C_n$ (cyclic group of order n): K. F. Roth 1953 — $X = o(n)$,

(K. O'Bryant 2011) $n2^{-\sqrt{8\log_2 n}} \leqslant X \leqslant C\dfrac{(\log\log n)^4}{\log n}n$ (T. Bloom 2016

$G = C_p^n$: $X = o(|G|^{1-\delta})$, $p = 4$: E. Croot, V. Lev, P. Pach (2016), even without semi-trivial progressions $a \cdot a = b^2$

Progressions

G is a group,nontrivial progression in G: $ac = b^2$, a, b, c not all equal
(warning: $ba^{-1} = cb^{-1}$ is a different condition)
Maximal size X of a progression-free set in a given finite group G?
$G = C_n$ (cyclic group of order n): K. F. Roth 1953 — $X = o(n)$,

(K. O'Bryant 2011) $n2^{-\sqrt{8\log_2 n}} \leqslant X \leqslant C\frac{(\log\log n)^4}{\log n} n$ (T. Bloom 2016

$G = C_p^n$: $X = o(|G|^{1-\delta})$, $p = 4$: E. Croot, V. Lev, P. Pach (2016),
even without semi-trivial progressions $a \cdot a = b^2$
p odd prime: J. Ellenberg, D. Gijswijt (2016, soon after)

Progressions

G is a group,nontrivial progression in G: $ac = b^2$, a, b, c not all equal
(warning: $ba^{-1} = cb^{-1}$ is a different condition)
Maximal size X of a progression-free set in a given finite group G?
$G = C_n$ (cyclic group of order n): K. F. Roth 1953 — $X = o(n)$,

$$\text{(K. O'Bryant 2011)}\ \ n2^{-\sqrt{8\log_2 n}} \leqslant X \leqslant C\frac{(\log\log n)^4}{\log n}n\ \ \text{(T. Bloom 2016)}$$

$G = C_p^n$: $X = o(|G|^{1-\delta})$, $p = 4$: E. Croot, V. Lev, P. Pach (2016), even without semi-trivial progressions $a \cdot a = b^2$
p odd prime: J. Ellenberg, D. Gijswijt (2016, soon after)
Proof ingredients: *polynomial method* (in spirit of Alon's Combinatorial Nullstellensatz),

Progressions

G is a group,nontrivial progression in G: $ac = b^2$, a, b, c not all equal
(warning: $ba^{-1} = cb^{-1}$ is a different condition)
Maximal size X of a progression-free set in a given finite group G?
$G = C_n$ (cyclic group of order n): K. F. Roth 1953 — $X = o(n)$,

(K. O'Bryant 2011) $n2^{-\sqrt{8\log_2 n}} \leqslant X \leqslant C\frac{(\log\log n)^4}{\log n} n$ (T. Bloom 2016)

$G = C_p^n$: $X = o(|G|^{1-\delta})$, $p = 4$: E. Croot, V. Lev, P. Pach (2016), even without semi-trivial progressions $a \cdot a = b^2$
p odd prime: J. Ellenberg, D. Gijswijt (2016, soon after)
Proof ingredients: *polynomial method* (in spirit of Alon's Combinatorial Nullstellensatz),*linear algebraic* dimension reasoning

Progressions

G is a group,nontrivial progression in G: $ac = b^2$, a, b, c not all equal
(warning: $ba^{-1} = cb^{-1}$ is a different condition)
Maximal size X of a progression-free set in a given finite group G?
$G = C_n$ (cyclic group of order n): K. F. Roth 1953 — $X = o(n)$,

$$\text{(K. O'Bryant 2011)} \;\; n2^{-\sqrt{8\log_2 n}} \leqslant X \leqslant C\frac{(\log\log n)^4}{\log n}n \;\; \text{(T. Bloom 2016)}$$

$G = C_p^n$: $X = o(|G|^{1-\delta})$, $p = 4$: E. Croot, V. Lev, P. Pach (2016), even without semi-trivial progressions $a \cdot a = b^2$
p odd prime: J. Ellenberg, D. Gijswijt (2016, soon after)
Proof ingredients: *polynomial method* (in spirit of Alon's Combinatorial Nullstellensatz),*linear algebraic* dimension reasoning and *law of large numbers*

Multiplicative matchings

Multiplicative matchings

The set of ordered triples (x_i, y_i, z_i): $x_i y_j z_k = 1 \Leftrightarrow i = j = k$

Multiplicative matchings

The set of ordered triples (x_i, y_i, z_i): $x_i y_j z_k = 1 \Leftrightarrow i = j = k$
Progression-free set A: (a, a, a^{-2}).

Multiplicative matchings

The set of ordered triples (x_i, y_i, z_i): $x_i y_j z_k = 1 \Leftrightarrow i = j = k$
Progression-free set A: (a, a, a^{-2}).
X (max progession-free set) $\leqslant Y$ (max multiplicative matching)

Multiplicative matchings

The set of ordered triples (x_i, y_i, z_i): $x_i y_j z_k = 1 \Leftrightarrow i = j = k$
Progression-free set A: (a, a, a^{-2}).
X (max progession-free set) $\leqslant Y$ (max multiplicative matching)
still $Y = o(|G|^{1-\delta})$ for $G = C_p^n$

Multiplicative matchings

The set of ordered triples (x_i, y_i, z_i): $x_i y_j z_k = 1 \Leftrightarrow i = j = k$
Progression-free set A: (a, a, a^{-2}).
X (max progession-free set) $\leqslant Y$ (max multiplicative matching)
still $Y = o(|G|^{1-\delta})$ for $G = C_p^n$
proof: literally the same

Multiplicative matchings

The set of ordered triples (x_i, y_i, z_i): $x_i y_j z_k = 1 \Leftrightarrow i = j = k$
Progression-free set A: (a, a, a^{-2}).
X (max progession-free set) $\leqslant Y$ (max multiplicative matching)
still $Y = o(|G|^{1-\delta})$ for $G = C_p^n$
proof: literally the same
important feature: sharp value of δ for fixed p and large n (R. Kleinberg, W. Sawin, D. Speyer; arbitrary p: finished by S. Norin and L. Pebody)

Ellenberg's refinement

Ellenberg's refinement

For all subsets $A, B \subset G$, there are $A_1 \subset A$, $B_1 \subset B$:
$AB \subset A_1 B \cup AB_1$ and $|A_1| + |B_1| \leqslant Z$.

Ellenberg's refinement

For all subsets $A, B \subset G$, there are $A_1 \subset A$, $B_1 \subset B$:
$AB \subset A_1 B \cup AB_1$ and $|A_1| + |B_1| \leqslant Z$.
Max multiplicative matching $\{(x_i, y_i, z_i)\}$: $Y \leqslant Z$

Ellenberg's refinement

For all subsets $A, B \subset G$, there are $A_1 \subset A$, $B_1 \subset B$:
$AB \subset A_1 B \cup AB_1$ and $|A_1| + |B_1| \leqslant Z$.
Max multiplicative matching $\{(x_i, y_i, z_i)\}$: $Y \leqslant Z$
$A = \{x_i\}$, $B = \{y_j\}$,

Ellenberg's refinement

For all subsets $A, B \subset G$, there are $A_1 \subset A$, $B_1 \subset B$:
$AB \subset A_1 B \cup AB_1$ and $|A_1| + |B_1| \leqslant Z$.
Max multiplicative matching $\{(x_i, y_i, z_i)\} : \ Y \leqslant Z$
$A = \{x_i\}$, $B = \{y_j\}$,for any k: $z_k^{-1} = x_k y_k = x_i y_j$ for $x_i \in A_1$ or $y_j \in B_1$.

Ellenberg's refinement

For all subsets $A, B \subset G$, there are $A_1 \subset A$, $B_1 \subset B$:
$AB \subset A_1 B \cup AB_1$ and $|A_1| + |B_1| \leqslant Z$.
Max multiplicative matching $\{(x_i, y_i, z_i)\} :\ Y \leqslant Z$
$A = \{x_i\}$, $B = \{y_j\}$,for any k: $z_k^{-1} = x_k y_k = x_i y_j$ for $x_i \in A_1$ or $y_j \in B_1$.Thus $x_k \in A_1$ or $y_k \in B_1$.

Ellenberg's refinement

For all subsets $A, B \subset G$, there are $A_1 \subset A$, $B_1 \subset B$:
$AB \subset A_1 B \cup AB_1$ and $|A_1| + |B_1| \leqslant Z$.
Max multiplicative matching $\{(x_i, y_i, z_i)\}$: $Y \leqslant Z$
$A = \{x_i\}$, $B = \{y_j\}$,for any k: $z_k^{-1} = x_k y_k = x_i y_j$ for $x_i \in A_1$ or $y_j \in B_1$.Thus $x_k \in A_1$ or $y_k \in B_1$. $Z = |A_1| + |B_1| \geqslant Y$

Ellenberg's refinement

For all subsets $A, B \subset G$, there are $A_1 \subset A$, $B_1 \subset B$:
$AB \subset A_1 B \cup AB_1$ and $|A_1| + |B_1| \leqslant Z$.
Max multiplicative matching $\{(x_i, y_i, z_i)\}$: $Y \leqslant Z$
$A = \{x_i\}$, $B = \{y_j\}$,for any k: $z_k^{-1} = x_k y_k = x_i y_j$ for $x_i \in A_1$ or $y_j \in B_1$.Thus $x_k \in A_1$ or $y_k \in B_1$. $Z = |A_1| + |B_1| \geqslant Y$
Ellenberg's theorem (2016): Z still does not exceed the discussed bound for X and Y

Ellenberg's refinement

For all subsets $A, B \subset G$, there are $A_1 \subset A$, $B_1 \subset B$:
$AB \subset A_1 B \cup AB_1$ and $|A_1| + |B_1| \leqslant Z$.
Max multiplicative matching $\{(x_i, y_i, z_i)\}$: $Y \leqslant Z$
$A = \{x_i\}$, $B = \{y_j\}$,for any k: $z_k^{-1} = x_k y_k = x_i y_j$ for $x_i \in A_1$ or $y_j \in B_1$.Thus $x_k \in A_1$ or $y_k \in B_1$. $Z = |A_1| + |B_1| \geqslant Y$
Ellenberg's theorem (2016): Z still does not exceed the discussed bound for X and Y
Proof: the same polynomial and probabilistic parts, but more involved linear algebraic lemma by R. Meshulam (1985)

Group rings

Group rings

G is a group, K is a field

Group rings

G is a group, K is a field

$$K[G] = \left\{ z = \sum c_g \cdot g : c_g \in K, g \in G \right\}$$

Group rings

G is a group, K is a field

$$K[G] = \left\{ z = \sum c_g \cdot g : c_g \in K, g \in G \right\}$$

multiplication: natural (convolution of functions on G)

Group rings

G is a group, K is a field

$$K[G] = \left\{ z = \sum c_g \cdot g : c_g \in K, g \in G \right\}$$

multiplication: natural (convolution of functions on G)

$$supp(z) = \{g : c_g \neq 0\}$$

Group rings

G is a group, K is a field

$$K[G] = \left\{ z = \sum c_g \cdot g : c_g \in K, g \in G \right\}$$

multiplication: natural (convolution of functions on G)

$$supp(z) = \{g : c_g \neq 0\}$$

$$supp(z_1 z_2) \subset supp(z_1) \cdot supp(z_2)$$

Group rings

G is a group, K is a field

$$K[G] = \left\{ z = \sum c_g \cdot g : c_g \in K, g \in G \right\}$$

multiplication: natural (convolution of functions on G)

$$supp(z) = \{g : c_g \neq 0\}$$

$$supp(z_1 z_2) \subset supp(z_1) \cdot supp(z_2)$$

G linearly acts on $\mathbb{C}[G]$ by multiplications

Group rings

G is a group, K is a field

$$K[G] = \left\{ z = \sum c_g \cdot g : c_g \in K, g \in G \right\}$$

multiplication: natural (convolution of functions on G)

$$supp(z) = \{g : c_g \neq 0\}$$

$$supp(z_1 z_2) \subset supp(z_1) \cdot supp(z_2)$$

G linearly acts on $\mathbb{C}[G]$ by multiplications
$\mathbb{C}[G] \sim$ representation theory of G

Nilpotent subspaces

Nilpotent subspaces

$X_0, \ldots, X_k$ — K-linear subspaces of $K[G]$, $X_0 \cdot X_1 \cdot \ldots \cdot X_k = 0$

Nilpotent subspaces

$X_0, \ldots, X_k$ — K-linear subspaces of $K[G]$, $X_0 \cdot X_1 \cdot \ldots \cdot X_k = 0$
$t_i = \operatorname{codim} X_i$

Nilpotent subspaces

$X_0, \ldots, X_k$ — K-linear subspaces of $K[G]$, $X_0 \cdot X_1 \cdot \ldots \cdot X_k = 0$
$t_i = \operatorname{codim} X_i$
Theorem. $A_1, \ldots, A_k$ — arbitrary subsets of G. Then there exist subsets $B_i \subset A_i$, $i = 1, \ldots, k$, and $C \subset G$ such that $|C| \leqslant t_0$, $|B_i| \leqslant t_i$ for all $i = 1, \ldots, k$, and

$$A_1 A_2 \cdot \ldots \cdot A_k \subset C \cup B_1 A_2 \cdot \ldots \cdot A_k \cup A_1 B_2 \cdot \ldots \cdot A_k \cup \ldots \cup A_1 A_2 \cdot \ldots \cdot A_{k-1} B_k.$$

Leaders and outsiders

Leaders and outsiders

A — linearly ordered, $|A| = d$, like $A = \{1, 2, \ldots, d\}$

Leaders and outsiders

A — linearly ordered, $|A| = d$, like $A = \{1, 2, \ldots, d\}$

Leaders and outsiders

A — linearly ordered, $|A| = d$, like $A = \{1, 2, \ldots, d\}$
$z : A \to K$ a function, not identical 0

Leaders and outsiders

A — linearly ordered, $|A| = d$, like $A = \{1, 2, \ldots, d\}$
$z : A \to K$ a function, not identical 0
the leader $\ell(z)$ and the outsider $out(z)$ are the minimal, corr. maximal, $a \in A$ such that $z(a) \neq 0$.

Leaders and outsiders

A — linearly ordered, $|A| = d$, like $A = \{1, 2, \dots, d\}$
$z : A \to K$ a function, not identical 0
the leader $\ell(z)$ and the outsider $out(z)$ are the minimal, corr. maximal, $a \in A$ such that $z(a) \neq 0$.
Key lemma. Let $W \subset K^A$ be a linear subspace. Then there are exactly $\dim W$ different leaders of non-zero elements of W (and, of course, as many different outsiders)

Leaders and outsiders

A — linearly ordered, $|A| = d$, like $A = \{1, 2, \ldots, d\}$
$z : A \to K$ a function, not identical 0
the leader $\ell(z)$ and the outsider $out(z)$ are the minimal, corr. maximal, $a \in A$ such that $z(a) \neq 0$.

Key lemma. Let $W \subset K^A$ be a linear subspace. Then there are exactly $\dim W$ different leaders of non-zero elements of W (and, of course, as many different outsiders)

Proof. Gauss elimination.

Leaders and outsiders

A — linearly ordered, $|A| = d$, like $A = \{1, 2, \ldots, d\}$
$z : A \to K$ a function, not identical 0
the leader $\ell(z)$ and the outsider $out(z)$ are the minimal, corr. maximal, $a \in A$ such that $z(a) \neq 0$.

Key lemma. Let $W \subset K^A$ be a linear subspace. Then there are exactly $\dim W$ different leaders of non-zero elements of W (and, of course, as many different outsiders)

Proof. Gauss elimination. Find a base $y_1, \ldots, y_m$ in W with different leaders $a_1 < \cdots < a_m$.

Leaders and outsiders

A — linearly ordered, $|A| = d$, like $A = \{1, 2, \ldots, d\}$
$z : A \to K$ a function, not identical 0
the leader $\ell(z)$ and the outsider $out(z)$ are the minimal, corr. maximal, $a \in A$ such that $z(a) \neq 0$.
Key lemma. Let $W \subset K^A$ be a linear subspace. Then there are exactly $\dim W$ different leaders of non-zero elements of W (and, of course, as many different outsiders)
Proof. Gauss elimination. Find a base $y_1, \ldots, y_m$ in W with different leaders $a_1 < \cdots < a_m$. The leader of any non-zero element $z \in W$, $z = \sum c_i y_i$, equals a_j for $j = \min\{i : c_i \neq 0\}$.

Construction of small sets C and B_i's

Construction of small sets C and B_i's

W: space of functions f on $A_1 \times A_2 \times \ldots \times A_k$ of the form $f(a_1, \ldots, a_k) = \varphi(a_1 \ldots a_k)$, $\varphi : G \to K$

Construction of small sets C and B_i's

W: space of functions f on $A_1 \times A_2 \times \ldots \times A_k$ of the form
$f(a_1, \ldots, a_k) = \varphi(a_1 \ldots a_k)$, $\varphi : G \to K$
Let A_i be linearly ordered, then $A_1 \times \ldots \times A_k$ is lex-ordered

Construction of small sets C and B_i's

W: space of functions f on $A_1 \times A_2 \times \ldots \times A_k$ of the form
$f(a_1, \ldots, a_k) = \varphi(a_1 \ldots a_k)$, $\varphi : G \to K$
Let A_i be linearly ordered, then $A_1 \times \ldots \times A_k$ is lex-ordered
Consider the leaders of non-zero elements of W.

Construction of small sets C and B_i's

W: space of functions f on $A_1 \times A_2 \times \ldots \times A_k$ of the form $f(a_1, \ldots, a_k) = \varphi(a_1 \ldots a_k)$, $\varphi : G \to K$
Let A_i be linearly ordered, then $A_1 \times \ldots \times A_k$ is lex-ordered
Consider the leaders of non-zero elements of W. What we actually show: all but at most t_0 of these leaders may be covered by the sets $B_1 \times A_2 \times \ldots \times A_k$, $A_1 \times B_2 \times \ldots \times B_k$, $\ldots$, $A_1 \times A_2 \times \ldots \times A_{k-1} \times B_k$ for certain subsets $B_i \subset A_i$, $|B_i| \leqslant t_i$.

Construction of small sets C and B_i's

W: space of functions f on $A_1 \times A_2 \times \ldots \times A_k$ of the form $f(a_1, \ldots, a_k) = \varphi(a_1 \ldots a_k)$, $\varphi : G \to K$
Let A_i be linearly ordered, then $A_1 \times \ldots \times A_k$ is lex-ordered
Consider the leaders of non-zero elements of W. What we actually show: all but at most t_0 of these leaders may be covered by the sets $B_1 \times A_2 \times \ldots \times A_k$, $A_1 \times B_2 \times \ldots \times B_k$, $\ldots$, $A_1 \times A_2 \times \ldots \times A_{k-1} \times B_k$ for certain subsets $B_i \subset A_i$, $|B_i| \leqslant t_i$.
$W_0 \subset W$: $\sum \varphi(g) g^{-1} \in X_0$.

Construction of small sets C and B_i's

W: space of functions f on $A_1 \times A_2 \times \ldots \times A_k$ of the form $f(a_1, \ldots, a_k) = \varphi(a_1 \ldots a_k)$, $\varphi : G \to K$
Let A_i be linearly ordered, then $A_1 \times \ldots \times A_k$ is lex-ordered
Consider the leaders of non-zero elements of W. What we actually show: all but at most t_0 of these leaders may be covered by the sets $B_1 \times A_2 \times \ldots \times A_k$, $A_1 \times B_2 \times \ldots \times B_k$, $\ldots$, $A_1 \times A_2 \times \ldots \times A_{k-1} \times B_k$ for certain subsets $B_i \subset A_i$, $|B_i| \leqslant t_i$.
$W_0 \subset W$: $\sum \varphi(g)g^{-1} \in X_0$. $\dim W/W_0 \leqslant t_0$, thus by Key Lemma all but at most t_0 leaders of the elements of W are the leaders of the elements of W_0.

Construction of small sets C and B_i's

W: space of functions f on $A_1 \times A_2 \times \ldots \times A_k$ of the form $f(a_1, \ldots, a_k) = \varphi(a_1 \ldots a_k)$, $\varphi : G \to K$
Let A_i be linearly ordered, then $A_1 \times \ldots \times A_k$ is lex-ordered
Consider the leaders of non-zero elements of W. What we actually show: all but at most t_0 of these leaders may be covered by the sets $B_1 \times A_2 \times \ldots \times A_k$, $A_1 \times B_2 \times \ldots \times B_k$, $\ldots$, $A_1 \times A_2 \times \ldots \times A_{k-1} \times B_k$ for certain subsets $B_i \subset A_i$, $|B_i| \leqslant t_i$.
$W_0 \subset W$: $\sum \varphi(g) g^{-1} \in X_0$. $\dim W/W_0 \leqslant t_0$, thus by Key Lemma all but at most t_0 leaders of the elements of W are the leaders of the elements of W_0.
$K^{A_i} \subset K[G]$: span of A_i,

Construction of small sets C and B_i's

W: space of functions f on $A_1 \times A_2 \times \ldots \times A_k$ of the form $f(a_1, \ldots, a_k) = \varphi(a_1 \ldots a_k)$, $\varphi : G \to K$
Let A_i be linearly ordered, then $A_1 \times \ldots \times A_k$ is lex-ordered
Consider the leaders of non-zero elements of W. What we actually show: all but at most t_0 of these leaders may be covered by the sets $B_1 \times A_2 \times \ldots \times A_k$, $A_1 \times B_2 \times \ldots \times B_k$, $\ldots$, $A_1 \times A_2 \times \ldots \times A_{k-1} \times B_k$ for certain subsets $B_i \subset A_i$, $|B_i| \leqslant t_i$.
$W_0 \subset W$: $\sum \varphi(g)g^{-1} \in X_0$. $\dim W/W_0 \leqslant t_0$, thus by Key Lemma all but at most t_0 leaders of the elements of W are the leaders of the elements of W_0.
$K^{A_i} \subset K[G]$: span of A_i, the outsiders of $K^{A_i} \cap X_i$ take all but at most t_i values,

Construction of small sets C and B_i's

W: space of functions f on $A_1 \times A_2 \times \ldots \times A_k$ of the form $f(a_1, \ldots, a_k) = \varphi(a_1 \ldots a_k)$, $\varphi : G \to K$
Let A_i be linearly ordered, then $A_1 \times \ldots \times A_k$ is lex-ordered
Consider the leaders of non-zero elements of W. What we actually show: all but at most t_0 of these leaders may be covered by the sets $B_1 \times A_2 \times \ldots \times A_k$, $A_1 \times B_2 \times \ldots \times B_k$, $\ldots$, $A_1 \times A_2 \times \ldots \times A_{k-1} \times B_k$ for certain subsets $B_i \subset A_i$, $|B_i| \leqslant t_i$.
$W_0 \subset W$: $\sum \varphi(g) g^{-1} \in X_0$. $\dim W/W_0 \leqslant t_0$, thus by Key Lemma all but at most t_0 leaders of the elements of W are the leaders of the elements of W_0.
$K^{A_i} \subset K[G]$: span of A_i, the outsiders of $K^{A_i} \cap X_i$ take all but at most t_i values, let $B_i \subset A_i$ consist of *non-outsiders* of the elements from $K^{A_i} \cap X_i$

Proof

Proof

Assume the contrary:

Proof

Assume the contrary: $\sum \varphi(g)g^{-1} \in X_0$, the leader $(c_1, \ldots, c_k)$ of a function $\varphi(a_1 \ldots a_k)$ on $A_1 \times \ldots \times A_k$ satisfies $c_i \notin B_i$ for all $i = 1, \ldots, k$.

Proof

Assume the contrary: $\sum \varphi(g)g^{-1} \in X_0$, the leader $(c_1, \dots, c_k)$ of a function $\varphi(a_1 \dots a_k)$ on $A_1 \times \dots \times A_k$ satisfies $c_i \notin B_i$ for all $i = 1, \dots, k$. Exist $\eta_i \in K^{A_i} \cap X_i$ with outsiders $out(\eta_i) = c_i$.

Proof

Assume the contrary: $\sum \varphi(g)g^{-1} \in X_0$, the leader $(c_1, \ldots, c_k)$ of a function $\varphi(a_1 \ldots a_k)$ on $A_1 \times \ldots \times A_k$ satisfies $c_i \notin B_i$ for all $i = 1, \ldots, k$. Exist $\eta_i \in K^{A_i} \cap X_i$ with outsiders $out(\eta_i) = c_i$. Look at the constant term of the product

$$[1] \left(\sum \varphi(g)g^{-1}\right) \cdot \eta_1 \cdot \eta_2 \cdot \ldots \cdot \eta_k = 0.$$

Proof

Assume the contrary: $\sum \varphi(g)g^{-1} \in X_0$, the leader $(c_1, \dots, c_k)$ of a function $\varphi(a_1 \dots a_k)$ on $A_1 \times \dots \times A_k$ satisfies $c_i \notin B_i$ for all $i = 1, \dots, k$. Exist $\eta_i \in K^{A_i} \cap X_i$ with outsiders $out(\eta_i) = c_i$. Look at the constant term of the product

$$[1] \left(\sum \varphi(g)g^{-1}\right) \cdot \eta_1 \cdot \eta_2 \cdot \ldots \cdot \eta_k = 0.$$

It equals

$$\sum_{a_i \in A_i} \varphi(a_1 \dots a_k)[a_1]\eta_1[a_2]\eta_2 \dots [a_k]\eta_k,$$

Proof

Assume the contrary: $\sum \varphi(g)g^{-1} \in X_0$, the leader $(c_1, \ldots, c_k)$ of a function $\varphi(a_1 \ldots a_k)$ on $A_1 \times \ldots \times A_k$ satisfies $c_i \notin B_i$ for all $i = 1, \ldots, k$. Exist $\eta_i \in K^{A_i} \cap X_i$ with outsiders $out(\eta_i) = c_i$. Look at the constant term of the product

$$[1] \left(\sum \varphi(g)g^{-1}\right) \cdot \eta_1 \cdot \eta_2 \cdot \ldots \cdot \eta_k = 0.$$

It equals

$$\sum_{a_i \in A_i} \varphi(a_1 \ldots a_k)[a_1]\eta_1[a_2]\eta_2 \ldots [a_k]\eta_k,$$

and by the lexicographic reasoning the onliest non-zero summand is

$$\varphi(c_1 \ldots c_k)[c_1]\eta_1[c_2]\eta_2 \ldots [c_k]\eta_k \neq 0,$$

a contradiction.

Example 1: Abelian p-groups

Example 1: Abelian p-groups

Let p be a prime. Let $G = \prod_{i=1}^{n} C_{N_i}$ be a finite Abelian p-group with n generators $g_1, \ldots, g_n$, g_i generates C_{N_i}, each N_i is a power of p.

Example 1: Abelian p-groups

Let p be a prime. Let $G = \prod_{i=1}^{n} C_{N_i}$ be a finite Abelian p-group with n generators $g_1, \ldots, g_n$, g_i generates C_{N_i}, each N_i is a power of p. $\mathbb{F}_p[G]$ is generated by the products $\prod(1 - g_i)^{m_i}$, where $m_i \in \{0, 1, \ldots, N_i \ - \ 1\}$.

Example 1: Abelian p-groups

Let p be a prime. Let $G = \prod_{i=1}^{n} C_{N_i}$ be a finite Abelian p-group with n generators $g_1, \ldots, g_n$, g_i generates C_{N_i}, each N_i is a power of p. $\mathbb{F}_p[G]$ is generated by the products $\prod (1 - g_i)^{m_i}$, where $m_i \in \{0, 1, \ldots, N_i \ - \ 1\}$.Fix positive parameters $\lambda_1, \ldots, \lambda_n$. Consider the subspace generated by monomials for which

$$\sum_{j=1}^{n} \lambda_j \left(\frac{m_j}{N_j - 1} - \frac{1}{3} \right) > 0$$

Example 1: Abelian p-groups

Let p be a prime. Let $G = \prod_{i=1}^{n} C_{N_i}$ be a finite Abelian p-group with n generators $g_1, \ldots, g_n$, g_i generates C_{N_i}, each N_i is a power of p. $\mathbb{F}_p[G]$ is generated by the products $\prod(1-g_i)^{m_i}$, where $m_i \in \{0, 1, \ldots, N_i \ - \ 1\}$.Fix positive parameters $\lambda_1, \ldots, \lambda_n$. Consider the subspace generated by monomials for which

$$\sum_{j=1}^{n} \lambda_j \left(\frac{m_j}{N_j - 1} - \frac{1}{3} \right) > 0$$

Any product $f_1 f_2 f_3$ for $f_i \in X$ has some $1 - g_j$ in a power strictly greater than $N_j - 1$, but $(1-g_j)^{N_j} = 0$.

Example 1: Abelian p-groups

Let p be a prime. Let $G = \prod_{i=1}^{n} C_{N_i}$ be a finite Abelian p-group with n generators $g_1, \dots, g_n$, g_i generates C_{N_i}, each N_i is a power of p. $\mathbb{F}_p[G]$ is generated by the products $\prod (1-g_i)^{m_i}$, where $m_i \in \{0, 1, \dots, N_i \ - \ 1\}$.Fix positive parameters $\lambda_1, \dots, \lambda_n$. Consider the subspace generated by monomials for which

$$\sum_{j=1}^{n} \lambda_j \left(\frac{m_j}{N_j - 1} - \frac{1}{3} \right) > 0$$

Any product $f_1 f_2 f_3$ for $f_i \in X$ has some $1 - g_j$ in a power strictly greater than $N_j - 1$, but $(1-g_j)^{N_j} = 0$. Chernoff bound:

$$\operatorname{codim} X \leqslant \prod_i \kappa(N_i),\ \kappa(N) = \min_{x>0} x^{-(N-1)/3}(1+x+\dots+x^{N-1}) < N$$

Example 1: Abelian p-groups

Let p be a prime. Let $G = \prod_{i=1}^{n} C_{N_i}$ be a finite Abelian p-group with n generators $g_1, \ldots, g_n$, g_i generates C_{N_i}, each N_i is a power of p. $\mathbb{F}_p[G]$ is generated by the products $\prod (1-g_i)^{m_i}$, where $m_i \in \{0, 1, \ldots, N_i \ - \ 1\}$.Fix positive parameters $\lambda_1, \ldots, \lambda_n$. Consider the subspace generated by monomials for which

$$\sum_{j=1}^{n} \lambda_j \left(\frac{m_j}{N_j - 1} - \frac{1}{3} \right) > 0$$

Any product $f_1 f_2 f_3$ for $f_i \in X$ has some $1 - g_j$ in a power strictly greater than $N_j - 1$, but $(1-g_j)^{N_j} = 0$. Chernoff bound:

$$\operatorname{codim} X \leqslant \prod_i \kappa(N_i),\ \kappa(N) = \min_{x>0} x^{-(N-1)/3}(1+x+\cdots+x^{N-1}) < N$$

For C_p^n the same estimate that polynomial method (E. Croot – V. Lev – P. Pach, J. Ellenberg – D. Gijswijt) gives.

Example 1: Abelian p-groups

Let p be a prime. Let $G = \prod_{i=1}^{n} C_{N_i}$ be a finite Abelian p-group with n generators $g_1, \dots, g_n$, g_i generates C_{N_i}, each N_i is a power of p. $\mathbb{F}_p[G]$ is generated by the products $\prod(1-g_i)^{m_i}$, where $m_i \in \{0, 1, \dots, N_i \ - \ 1\}$.Fix positive parameters $\lambda_1, \dots, \lambda_n$. Consider the subspace generated by monomials for which

$$\sum_{j=1}^{n} \lambda_j \left(\frac{m_j}{N_j - 1} - \frac{1}{3} \right) > 0$$

Any product $f_1 f_2 f_3$ for $f_i \in X$ has some $1 - g_j$ in a power strictly greater than $N_j - 1$, but $(1-g_j)^{N_j} = 0$. Chernoff bound:

$$\operatorname{codim} X \leqslant \prod_i \kappa(N_i),\ \kappa(N) = \min_{x>0} x^{-(N-1)/3}(1+x+\dots+x^{N-1}) < N$$

For C_p^n the same estimate that polynomial method (E. Croot – V. Lev – P. Pach, J. Ellenberg – D. Gijswijt) gives. CLP constant for C_4^n equals $\kappa(4)$.

Example 1: Abelian p-groups

Let p be a prime. Let $G = \prod_{i=1}^{n} C_{N_i}$ be a finite Abelian p-group with n generators $g_1, \ldots, g_n$, g_i generates C_{N_i}, each N_i is a power of p. $\mathbb{F}_p[G]$ is generated by the products $\prod(1-g_i)^{m_i}$, where $m_i \in \{0, 1, \ldots, N_i \ - \ 1\}$.Fix positive parameters $\lambda_1, \ldots, \lambda_n$. Consider the subspace generated by monomials for which

$$\sum_{j=1}^{n} \lambda_j \left(\frac{m_j}{N_j - 1} - \frac{1}{3} \right) > 0$$

Any product $f_1 f_2 f_3$ for $f_i \in X$ has some $1 - g_j$ in a power strictly greater than $N_j - 1$, but $(1-g_j)^{N_j} = 0$. Chernoff bound:

$$\operatorname{codim} X \leqslant \prod_i \kappa(N_i),\ \kappa(N) = \min_{x>0} x^{-(N-1)/3}(1+x+\cdots+x^{N-1}) < N$$

For C_p^n the same estimate that polynomial method (E. Croot – V. Lev – P. Pach, J. Ellenberg – D. Gijswijt) gives. CLP constant for C_4^n equals $\kappa(4)$. Other proofs for $\prod C_{p^r}$: W. Sawin, E. Naslund (binomials divisibility), D. Speyer (Witt vectors).

Example 2: Unitriangular matrices

Example 2: Unitriangular matrices

$G = UT(n, \mathbb{F}_p)$, $|G| = p^{n(n-1)/2}$.

Example 2: Unitriangular matrices

$G = UT(n, \mathbb{F}_p)$, $|G| = p^{n(n-1)/2}$.
$g_{ij} = id + e_{ij}$, $i < j$;

Example 2: Unitriangular matrices

$G = UT(n, \mathbb{F}_p)$, $|G| = p^{n(n-1)/2}$.
$g_{ij} = id + e_{ij}$, $i < j$; each element of G has unique representation

$$g_{n-1,n}^{\alpha_{n-1,n}} g_{n-2,n}^{\alpha_{n-2,n}} \dots g_{1,2}^{\alpha_{1,2}}, 0 \leqslant \alpha_{i,j} \leqslant p-1.$$

Example 2: Unitriangular matrices

$G = UT(n, \mathbb{F}_p)$, $|G| = p^{n(n-1)/2}$.
$g_{ij} = id + e_{ij}$, $i < j$; each element of G has unique representation

$$g_{n-1,n}^{\alpha_{n-1,n}} g_{n-2,n}^{\alpha_{n-2,n}} \dots g_{1,2}^{\alpha_{1,2}}, 0 \leqslant \alpha_{i,j} \leqslant p-1.$$

g_{ij} and g_{kl} commute unless $j = k$ or $i = l$. In this case we have relations $g_{ij}g_{jl} = g_{jl}g_{ij}g_{il}$. $x_{ij} = g_{ij} - 1$, in $\mathbb{F}_p[G]$ we have $x_{ij}^p = 0$ and $\mathbb{F}_p[G]$ has a basis

$$x_{n-1,n}^{\alpha_{n-1,n}} x_{n-2,n}^{\alpha_{n-2,n}} \dots x_{1,2}^{\alpha_{1,2}}, 0 \leqslant \alpha_{i,j} \leqslant p-1.$$

Example 2: Unitriangular matrices

$G = UT(n, \mathbb{F}_p)$, $|G| = p^{n(n-1)/2}$.
$g_{ij} = id + e_{ij}$, $i < j$; each element of G has unique representation

$$g_{n-1,n}^{\alpha_{n-1,n}} g_{n-2,n}^{\alpha_{n-2,n}} \dots g_{1,2}^{\alpha_{1,2}}, 0 \leqslant \alpha_{i,j} \leqslant p-1.$$

g_{ij} and g_{kl} commute unless $j = k$ or $i = l$. In this case we have relations $g_{ij} g_{jl} = g_{jl} g_{ij} g_{il}$. $x_{ij} = g_{ij} - 1$, in $\mathbb{F}_p[G]$ we have $x_{ij}^p = 0$ and $\mathbb{F}_p[G]$ has a basis

$$x_{n-1,n}^{\alpha_{n-1,n}} x_{n-2,n}^{\alpha_{n-2,n}} \dots x_{1,2}^{\alpha_{1,2}}, 0 \leqslant \alpha_{i,j} \leqslant p-1.$$

If $i < j < l$ we have $(1 + x_{ij})(1 + x_{jl}) = (1 + x_{jl})(1 + x_{ij})(1 + x_{il})$, thus $x_{ij} x_{jl} = x_{jl} x_{ij} + x_{il} + x_{ij} x_{il} + x_{jl} x_{il} + x_{jl} x_{ij} x_{il}$.

Example 2: Unitriangular matrices

$G = UT(n, \mathbb{F}_p)$, $|G| = p^{n(n-1)/2}$.
$g_{ij} = id + e_{ij}$, $i < j$; each element of G has unique representation

$$g_{n-1,n}^{\alpha_{n-1,n}} g_{n-2,n}^{\alpha_{n-2,n}} \dots g_{1,2}^{\alpha_{1,2}}, 0 \leqslant \alpha_{i,j} \leqslant p-1.$$

g_{ij} and g_{kl} commute unless $j = k$ or $i = l$. In this case we have relations $g_{ij} g_{jl} = g_{jl} g_{ij} g_{il}$. $x_{ij} = g_{ij} - 1$, in $\mathbb{F}_p[G]$ we have $x_{ij}^p = 0$ and $\mathbb{F}_p[G]$ has a basis

$$x_{n-1,n}^{\alpha_{n-1,n}} x_{n-2,n}^{\alpha_{n-2,n}} \dots x_{1,2}^{\alpha_{1,2}}, 0 \leqslant \alpha_{i,j} \leqslant p-1.$$

If $i < j < l$ we have $(1 + x_{ij})(1 + x_{jl}) = (1 + x_{jl})(1 + x_{ij})(1 + x_{il})$, thus $x_{ij} x_{jl} = x_{jl} x_{ij} + x_{il} + x_{ij} x_{il} + x_{jl} x_{il} + x_{jl} x_{ij} x_{il}$.

Example 2: Unitriangular matrices

$G = UT(n, \mathbb{F}_p)$, $|G| = p^{n(n-1)/2}$.
$g_{ij} = id + e_{ij}$, $i < j$; each element of G has unique representation

$$g_{n-1,n}^{\alpha_{n-1,n}} g_{n-2,n}^{\alpha_{n-2,n}} \dots g_{1,2}^{\alpha_{1,2}}, 0 \leqslant \alpha_{i,j} \leqslant p-1.$$

g_{ij} and g_{kl} commute unless $j = k$ or $i = l$. In this case we have relations $g_{ij}g_{jl} = g_{jl}g_{ij}g_{il}$. $x_{ij} = g_{ij} - 1$, in $\mathbb{F}_p[G]$ we have $x_{ij}^p = 0$ and $\mathbb{F}_p[G]$ has a basis

$$x_{n-1,n}^{\alpha_{n-1,n}} x_{n-2,n}^{\alpha_{n-2,n}} \dots x_{1,2}^{\alpha_{1,2}}, 0 \leqslant \alpha_{i,j} \leqslant p-1.$$

If $i < j < l$ we have $(1 + x_{ij})(1 + x_{jl}) = (1 + x_{jl})(1 + x_{ij})(1 + x_{il})$, thus $x_{ij}x_{jl} = x_{jl}x_{ij} + x_{il} + x_{ij}x_{il} + x_{jl}x_{il} + x_{jl}x_{ij}x_{il}$. Define a degree of any word in alphabet $\{x_{ij}\}$'s as a sum of $(j - i)$ over all used letters.

Example 2: Unitriangular matrices

$G = UT(n, \mathbb{F}_p)$, $|G| = p^{n(n-1)/2}$.
$g_{ij} = id + e_{ij}$, $i < j$; each element of G has unique representation

$$g_{n-1,n}^{\alpha_{n-1,n}} g_{n-2,n}^{\alpha_{n-2,n}} \dots g_{1,2}^{\alpha_{1,2}}, 0 \leqslant \alpha_{i,j} \leqslant p-1.$$

g_{ij} and g_{kl} commute unless $j = k$ or $i = l$. In this case we have relations $g_{ij}g_{jl} = g_{jl}g_{ij}g_{il}$. $x_{ij} = g_{ij} - 1$, in $\mathbb{F}_p[G]$ we have $x_{ij}^p = 0$ and $\mathbb{F}_p[G]$ has a basis

$$x_{n-1,n}^{\alpha_{n-1,n}} x_{n-2,n}^{\alpha_{n-2,n}} \dots x_{1,2}^{\alpha_{1,2}}, 0 \leqslant \alpha_{i,j} \leqslant p-1.$$

If $i < j < l$ we have $(1 + x_{ij})(1 + x_{jl}) = (1 + x_{jl})(1 + x_{ij})(1 + x_{il})$, thus $x_{ij}x_{jl} = x_{jl}x_{ij} + x_{il} + x_{ij}x_{il} + x_{jl}x_{il} + x_{jl}x_{ij}x_{il}$. Define a degree of any word in alphabet $\{x_{ij}\}$'s as a sum of $(j - i)$ over all used letters. X: span of reduced monomials of degree strictly greater than $(p-1)(\sum_{i<j}(j-i))/3$.