On Counting Subsets over Finite Fields

Li Jiyou

Department of Mathematics, Shanghai Jiao Tong University

May 2011, Coding, Cryptography and Combinatorial Designs, Singapore

Outline

Subset Sum Problem (SSP)

- Let A be a finite abelian group and $D \subset A$, $|D| = n$.

Subset Sum Problem (SSP)

- Let A be a finite abelian group and $D \subset A$, $|D| = n$.
- For $1 \leq k \leq n$ and $b \in A$, define

$$N_D(k, b) = \#\{S \subseteq D | \sum_{a \in S} a = b\}.$$

Subset Sum Problem (SSP)

- Let A be a finite abelian group and $D \subset A$, $|D| = n$.
- For $1 \leq k \leq n$ and $b \in A$, define

$$N_D(k, b) = \#\{S \subseteq D | \sum_{a \in S} a = b\}.$$

Problem (SSP)

Determine if $N_D(k, b) > 0$ *for some* $1 \leq k \leq n$.

Computational Complexity of SSP

Theorem

*The Subset Sum Problem (**SSP**) is **NP**-hard.*

Computational Complexity of SSP

Theorem

*The Subset Sum Problem (**SSP**) is **NP**-hard.*

If $n = O(\log |A|)$, then **SSP** can be solved by a reduction to finding a short vector in a lattice;

Computational Complexity of SSP

Theorem

*The Subset Sum Problem (**SSP**) is **NP**-hard.*

If $n = O(\log |A|)$, then **SSP** can be solved by a reduction to finding a short vector in a lattice;

If $n = O(|A|^{\epsilon})$, then **SSP** can be solved in polynomial time using dynamic programming;

Computational Complexity of SSP

Theorem

*The Subset Sum Problem (**SSP**) is **NP**-hard.*

If $n = O(\log |A|)$, then **SSP** can be solved by a reduction to finding a short vector in a lattice;

If $n = O(|A|^{\epsilon})$, then **SSP** can be solved in polynomial time using dynamic programming;

It is the basis of public-key cryptosystems of knapsack type.

Counting version of SSP

Problem

How to compute $N_D(b) = \sum_{k=0}^{n} N_D(k, b)$, or more precisely, compute $N_D(k, b)$?

Counting version of SSP

Problem

How to compute $N_D(b) = \sum_{k=0}^{n} N_D(k, b)$, or more precisely, compute $N_D(k, b)$?

For example, Erdos and Heilbronn proved in 1964 that when A is a prime field Z_p and $n = p$,

$$N_D(b) = \frac{2^n}{p}(1 + o(p))$$

as $\frac{n^3}{p^2} \to \infty$ as $p \to \infty$.

Covering Version of SSP

Define $D^k = \{a_1 + a_2 + \cdots + a_k, a_i \in D, a_i \neq a_j, i \neq j\}$.

Problem

Determine if $D^k = A$.

A Typical Example

- Let $A = \mathbb{F}_{q^h}^* = \mathbb{F}_q[\alpha]^*$ and $D = \{\alpha + a | a \in \mathbb{F}_q\}$. Then

A Typical Example

- Let $A = \mathbb{F}_{q^h}^* = \mathbb{F}_q[\alpha]^*$ and $D = \{\alpha + a | a \in \mathbb{F}_q\}$. Then
- $N_D(k, b) > 0$ for any $b \in \mathbb{F}_{q^h}^*$ means that $D = \{\alpha + a | a \in \mathbb{F}_q\}$ is a generator set of $\mathbb{F}_{q^h}^*$;

A Typical Example

- Let $A = \mathbb{F}_{q^h}^* = \mathbb{F}_q[\alpha]^*$ and $D = \{\alpha + a | a \in \mathbb{F}_q\}$. Then
- $N_D(k, b) > 0$ for any $b \in \mathbb{F}_{q^h}^*$ means that $D = \{\alpha + a | a \in \mathbb{F}_q\}$ is a generator set of $\mathbb{F}_{q^h}^*$;
- Equivalently, each $b \in \mathbb{F}_{q^h}^*$ can be written to a product of k distinct elements in $D = \{\alpha + a | a \in \mathbb{F}_q\}$;

A Typical Example

- Let $A = \mathbb{F}_{q^h}^* = \mathbb{F}_q[\alpha]^*$ and $D = \{\alpha + a | a \in \mathbb{F}_q\}$. Then
- $N_D(k, b) > 0$ for any $b \in \mathbb{F}_{q^h}^*$ means that $D = \{\alpha + a | a \in \mathbb{F}_q\}$ is a generator set of $\mathbb{F}_{q^h}^*$;
- Equivalently, each $b \in \mathbb{F}_{q^h}^*$ can be written to a product of k distinct elements in $D = \{\alpha + a | a \in \mathbb{F}_q\}$;
- Note that $|D| = q$ is very small compared to $|A| = q^h$ when h is large;

A Typical Example

- Let $A = \mathbb{F}_{q^h}^* = \mathbb{F}_q[\alpha]^*$ and $D = \{\alpha + a | a \in \mathbb{F}_q\}$. Then
- $N_D(k, b) > 0$ for any $b \in \mathbb{F}_{q^h}^*$ means that $D = \{\alpha + a | a \in \mathbb{F}_q\}$ is a generator set of $\mathbb{F}_{q^h}^*$;
- Equivalently, each $b \in \mathbb{F}_{q^h}^*$ can be written to a product of k distinct elements in $D = \{\alpha + a | a \in \mathbb{F}_q\}$;
- Note that $|D| = q$ is very small compared to $|A| = q^h$ when h is large;
- This is a basic problem in computational finite field theory;

A Typical Example

- Let $A = \mathbb{F}^*_{q^h} = \mathbb{F}_q[\alpha]^*$ and $D = \{\alpha + a | a \in \mathbb{F}_q\}$. Then
- $N_D(k, b) > 0$ for any $b \in \mathbb{F}^*_{q^h}$ means that $D = \{\alpha + a | a \in \mathbb{F}_q\}$ is a generator set of $\mathbb{F}^*_{q^h}$;
- Equivalently, each $b \in \mathbb{F}^*_{q^h}$ can be written to a product of k distinct elements in $D = \{\alpha + a | a \in \mathbb{F}_q\}$;
- Note that $|D| = q$ is very small compared to $|A| = q^h$ when h is large;
- This is a basic problem in computational finite field theory;
- It also arises from graph theory and number theoretic algorithms and has significant application in coding theory.

Chung's construction

- $V(G) = A$;

Chung's construction

- $V(G) = A$;
- $\forall \beta_1, \beta_2 \in V(G)$, $(\beta_1, \beta_2) \in E(G)$ iff $\beta_1/\beta_2 \in D$;

Chung's construction

- $V(G) = A$;
- $\forall \beta_1, \beta_2 \in V(G)$, $(\beta_1, \beta_2) \in E(G)$ iff $\beta_1/\beta_2 \in D$;
- $G = G(h, q, \alpha)$ is called a $q-$difference graph.

Chung's construction

- $V(G) = A$;
- $\forall \beta_1, \beta_2 \in V(G)$, $(\beta_1, \beta_2) \in E(G)$ iff $\beta_1/\beta_2 \in D$;
- $G = G(h, q, \alpha)$ is called a $q-$difference graph.
- $G = G(h, q, \alpha)$ are good expanders with small diameters;

Chung's construction

- $V(G) = A$;
- $\forall \beta_1, \beta_2 \in V(G)$, $(\beta_1, \beta_2) \in E(G)$ iff $\beta_1/\beta_2 \in D$;
- $G = G(h, q, \alpha)$ is called a $q-$difference graph.
- $G = G(h, q, \alpha)$ are good expanders with small diameters;
- They are studied firstly by F. R. Chung, N. M. Katz, and more generally by W. C. Li and K. Q. Feng, etc.

Chung's construction

- $V(G) = A$;
- $\forall \beta_1, \beta_2 \in V(G)$, $(\beta_1, \beta_2) \in E(G)$ iff $\beta_1/\beta_2 \in D$;
- $G = G(h, q, \alpha)$ is called a $q-$difference graph.
- $G = G(h, q, \alpha)$ are good expanders with small diameters;
- They are studied firstly by F. R. Chung, N. M. Katz, and more generally by W. C. Li and K. Q. Feng, etc.
- Applications: connection networks; extremal graph theory; cryptography; computational complexity, etc.

Geometric Examples

Problem

For which k, m, the following variety defined over $\mathbf{F}_q$ has a rational point:

$$\begin{aligned} f_1(x_1, x_2, \cdots, x_k) &= b_1; \\ f_2(x_1, x_2, \cdots, x_k) &= b_2; \\ \cdots, \cdots; \\ f_m(x_1, x_2, \cdots, x_k) &= b_m; \\ x_i - x_j &\neq 0. \end{aligned}$$

A Concrete Geometric Example

Problem

$$\sum_{i=1}^{k} x_i = b_1,$$

$$\sum_{1\le i_1<i_2\le k} x_{i_1}x_{i_2} = b_2,$$

$$\cdots,$$

$$\sum_{1\le i_1<i_2<\cdots<i_m\le k} x_{i_1}\cdots x_{i_m} = b_m,$$

$$x_i - x_j \neq 0 \ (i \neq j), x_i \in \mathbf{F}_q \ ;$$

A Concrete Geometric Example

For which k and n, there is a k-subset $S \subseteq \mathbf{F}_q$ such that:

$$\sum_{a \in S} a = b_1,$$

$$\sum_{\{a,b\} \subseteq S} ab = b_2,$$

$$\cdots,$$

$$\sum_{\{a,b,\cdots,c\} \subseteq \in S} ab \cdots c = b_m.$$

A Basic Example

- We note that

$$N_D(k,b) = \#\{(x_1,\cdots,x_k) | x_1+\cdots+x_k = b, x_i \in D, x_i \neq x_j, \forall i \neq j\};$$

A Basic Example

- We note that

$$N_D(k,b) = \#\{(x_1,\cdots,x_k) | x_1+\cdots+x_k = b, x_i \in D, x_i \neq x_j, \forall i \neq j\};$$

- Let $A = \mathbb{F}_q$ and $D = A$;

A Basic Example

- We note that

$$N_D(k,b) = \#\{(x_1,\cdots,x_k) | x_1+\cdots+x_k = b, x_i \in D, x_i \neq x_j, \forall i \neq j\};$$

- Let $A = \mathbb{F}_q$ and $D = A$;
- Let X be the number of solutions of the equation

$$x_1 + x_2 + \cdots + x_k = b, x_i \in \mathbb{F}_q;$$

A Basic Example

- We note that

$$N_D(k,b) = \#\{(x_1,\cdots,x_k)|x_1+\cdots+x_k = b, x_i \in D, x_i \neq x_j, \forall i \neq j\};$$

- Let $A = \mathbb{F}_q$ and $D = A$;
- Let X be the number of solutions of the equation

$$x_1 + x_2 + \cdots + x_k = b, x_i \in \mathbb{F}_q;$$

- Let X_{ij} be the number of solutions of the equation

$$x_1 + x_2 + \cdots + x_k = b, x_i \in \mathbb{F}_q, x_i = x_j;$$

A Basic Example

- We note that

$$N_D(k,b) = \#\{(x_1,\cdots,x_k) | x_1+\cdots+x_k = b, x_i \in D, x_i \neq x_j, \forall i \neq j\};$$

- Let $A = \mathbb{F}_q$ and $D = A$;
- Let X be the number of solutions of the equation

$$x_1 + x_2 + \cdots + x_k = b, x_i \in \mathbb{F}_q;$$

- Let X_{ij} be the number of solutions of the equation

$$x_1 + x_2 + \cdots + x_k = b, x_i \in \mathbb{F}_q, x_i = x_j;$$

- We have that

$$N_{\mathbb{F}_q}(k,b) = |\bigcap_{1\le i<j\le k} \overline{X_{ij}}|.$$

The Inclusion-exclusion Sieving

- We have the classical inclusion-exclusion sieving

$$
\begin{aligned}
|\overline{X}| &= |\bigcap_{1\le i<j\le k} \overline{X_{ij}}| \\
&= |X| - \sum_{1\le i<j\le k} |X_{ij}| + \sum_{1\le i<j\le k, 1\le s<t\le k, (i,j)\ne(s,t)} |X_{ij} \bigcap X_{st}| \\
&\quad - \cdots + (-1)^{\binom{k}{2}} |\bigcap_{1\le i<j\le k} X_{ij}|.
\end{aligned}
$$

The Inclusion-exclusion Sieving

- We have the classical inclusion-exclusion sieving

$$\begin{aligned} |\overline{X}| &= \Big|\bigcap_{1\le i<j\le k} \overline{X_{ij}}\Big| \\ &= |X| - \sum_{1\le i<j\le k} |X_{ij}| + \sum_{1\le i<j\le k, 1\le s<t\le k, (i,j)\neq(s,t)} |X_{ij} \bigcap X_{st}| \\ &\quad - \cdots + (-1)^{\binom{k}{2}} \Big|\bigcap_{1\le i<j\le k} X_{ij}\Big|. \end{aligned}$$

- There are totally $2^{\binom{k}{2}}$ terms!

Brun's Sieve

- $|\overline{X} \geq |X| - \sum_{1 \leq i < j \leq k} |X_{ij}|;$

Brun's Sieve

- $|\overline{X} \geq |X| - \sum_{1 \leq i < j \leq k} |X_{ij}|$;
- The number of terms is $1 + \binom{k}{2}$;

Brun’s Sieve

- $|\overline{X} \geq |X| - \sum_{1 \leq i < j \leq k} |X_{ij}|$;
- The number of terms is $1 + \binom{k}{2}$;
- The sum of remain $2^{\binom{k}{2}} - \binom{k}{2} - 1$ terms may cause a big error and thus a weak lower bound.

Bonferroni Inequality

- ......

$$|\overline{X} \geq |X| - \sum_{1\leq i<j\leq k} |X_{ij}| + \sum_{1\leq i<j\leq k, 1\leq s<t\leq k, (i,j)\neq(s,t)} |X_{ij} \bigcap X_{st}|$$
$$- \sum_{1\leq i<j\leq k, 1\leq s<t\leq k, 1\leq m<n\leq k} |X_{ij} \bigcap X_{st} \bigcap X_{mn}|;$$

Bonferroni Inequality

- ......

$$|\overline{X} \geq |X| - \sum_{1\leq i<j\leq k} |X_{ij}| + \sum_{1\leq i<j\leq k, 1\leq s<t\leq k, (i,j)\neq(s,t)} |X_{ij} \bigcap X_{st}|$$
$$- \sum_{1\leq i<j\leq k, 1\leq s<t\leq k, 1\leq m<n\leq k} |X_{ij} \bigcap X_{st} \bigcap X_{mn}|;$$

- The number of terms is $1 + \binom{k}{2} + \binom{\binom{k}{2}}{2} + \binom{\binom{k}{2}}{3}$;

Bonferroni Inequality

- $\cdots\cdots$

$$|\overline{X} \geq |X| - \sum_{1\leq i<j\leq k} |X_{ij}| + \sum_{1\leq i<j\leq k, 1\leq s<t\leq k, (i,j)\neq(s,t)} |X_{ij} \bigcap X_{st}|$$

$$- \sum_{1\leq i<j\leq k, 1\leq s<t\leq k, 1\leq m<n\leq k} |X_{ij} \bigcap X_{st} \bigcap X_{mn}|;$$

- The number of terms is $1 + \binom{k}{2} + \binom{\binom{k}{2}}{2} + \binom{\binom{k}{2}}{3}$;
- This lower bound may be better than Brun's sieve but more complicated .

Weighted Cases

- D is a nonempty set and $X \subseteq D^k$;

Weighted Cases

- D is a nonempty set and $X \subseteq D^k$;
- $f(x_1, x_2, \cdots, x_k)$ is a complex valued function;

Weighted Cases

- D is a nonempty set and $X \subseteq D^k$;
- $f(x_1, x_2, \cdots, x_k)$ is a complex valued function;
- Consider the summation

$$F = \sum_{\substack{\{x_1, x_2, \cdots, x_k\} \in X \\ \text{all } x_i \text{ are distinct}}} f(x_1, x_2, \cdots, x_k),$$

Weighted Cases

- D is a nonempty set and $X \subseteq D^k$;
- $f(x_1, x_2, \cdots, x_k)$ is a complex valued function;
- Consider the summation

$$F = \sum_{\substack{\{x_1, x_2, \cdots, x_k\} \in X \\ \text{all } x_i \text{ are distinct}}} f(x_1, x_2, \cdots, x_k),$$

- When $f(x_1, x_2, \cdots, x_k) \equiv 1$ we have $F = |\overline{X}|$;

Weighted Cases

- D is a nonempty set and $X \subseteq D^k$;
- $f(x_1, x_2, \cdots, x_k)$ is a complex valued function;
- Consider the summation

$$F = \sum_{\substack{\{x_1, x_2, \cdots, x_k\} \in X \\ \text{all } x_i \text{ are distinct}}} f(x_1, x_2, \cdots, x_k),$$

- When $f(x_1, x_2, \cdots, x_k) \equiv 1$ we have $F = |\overline{X}|$;
- Note that when $f(x_1, x_2, \cdots, x_k)$ is symmetric, we can regard F as a summation over certain subsets over D.

General Case of Inclusion-exclusion Sieving

$$
\begin{aligned}
F &= \sum_{(x_1,x_2,\cdots,x_k)\in\bigcap_{1\le i<j\le k}\overline{X_{ij}}} f(x_1,x_2,\cdots,x_k) \\
&= \sum_{(x_1,x_2,\cdots,x_k)\in X} f(x_1,x_2,\cdots,x_k) \\
&- \sum_{1\le i<j\le k}\ \sum_{(x_1,x_2,\cdots,x_k)\in X_{ij}} f(x_1,x_2,\cdots,x_k) \\
&+ \sum_{1\le i<j\le k,1\le s<t\le k,(i,j)\neq(s,t)}\ \sum_{(x_1,x_2,\cdots,x_k)\in X_{ij}\bigcap X_{st}} f(x_1,x_2,\cdots,x_k) \\
&\cdots \\
&+(-1)^{\binom{k}{2}} \sum_{(x_1,x_2,\cdots,x_k)\in\bigcap_{1\le i<j\le k}X_{ij}} f(x_1,x_2,\cdots,x_k).
\end{aligned}
$$

Notations

- For $\tau \in S_k$, suppose τ factors into disjoint cycles as

$$\tau = (i_1 i_2 \cdots i_{a_1})(j_1 j_2 \cdots j_{a_2}) \cdots (l_1 l_2 \cdots l_{a_s}), 1 \leq i \leq s.$$

Notations

- For $\tau \in S_k$, suppose τ factors into disjoint cycles as

$$\tau = (i_1 i_2 \cdots i_{a_1})(j_1 j_2 \cdots j_{a_2}) \cdots (l_1 l_2 \cdots l_{a_s}), 1 \leq i \leq s.$$

- Define

$$X_\tau = \left\{ (x_1, x_2, \cdots, x_k) \in X, x_{i_1} = \cdots = x_{i_{a_1}}, \cdots, x_{l_1} = \cdots = x_{l_{a_s}} \right\}.$$

The Formula

Theorem (J. Li and D. Wan, 2008)

Let $\overline{X}, X_\tau$ be defined as above. Then we have

$$|\overline{X}| = \sum_{\tau \in S_k} sign(\tau)|X_\tau|.$$

Symmetry

- The symmetric group S_k acts on D^k naturally by permuting coordinates.

Symmetry

- The symmetric group S_k acts on D^k naturally by permuting coordinates.
- For given $\tau \in S_k$ and $x = (x_1, x_2, \cdots, x_k) \in D^k$,

$$\tau \circ x = (x_{\tau(1)}, x_{\tau(2)}, \cdots, x_{\tau(k)}).$$

Symmetry

- The symmetric group S_k acts on D^k naturally by permuting coordinates.
- For given $\tau \in S_k$ and $x = (x_1, x_2, \cdots, x_k) \in D^k$,

$$\tau \circ x = (x_{\tau(1)}, x_{\tau(2)}, \cdots, x_{\tau(k)}).$$

- Let G be a subgroup of S_k. A subset $X \subset D^k$ is said to be G-symmetric if for any $x \in X$ and any $g \in G$, $g \circ x \in X$.

Symmetry

- The symmetric group S_k acts on D^k naturally by permuting coordinates.
- For given $\tau \in S_k$ and $x = (x_1, x_2, \cdots, x_k) \in D^k$,

$$\tau \circ x = (x_{\tau(1)}, x_{\tau(2)}, \cdots, x_{\tau(k)}).$$

- Let G be a subgroup of S_k. A subset $X \subset D^k$ is said to be G-symmetric if for any $x \in X$ and any $g \in G$, $g \circ x \in X$.
- In particular, a S_k-symmetric X is simply called symmetric.

Special Cases

Corollary

$$|\overline{X}| = \sum_{\tau \in G_k} sign(\tau) G(\tau) |X_\tau|,$$

where G_k is the set of G-conjugacy class of S_k and $G(\tau)$ is the orbit length of τ by G-conjugate action on S_k.

Special Case

Corollary

If X is symmetric, then

$$|X| = \sum_{\tau \in C_k} (-1)^{k-l(\tau)} C(\tau) |X_\tau|,$$

Special Case

Corollary

If X is symmetric, then

$$|X| = \sum_{\tau \in C_k} (-1)^{k-l(\tau)} C(\tau) |X_\tau|,$$

- The number of terms is $p(k) = 2^{O(\sqrt{k})}$.

Special Case 2

Corollary

If X is strongly symmetric, then we have

$$|\overline{X}| = \sum_{i=1}^{k} (-1)^{k-i} c(k,i) |X_i|,$$

where X_i is defined as X_{τ_i} for some $\tau_i \in S_k$ with $l(\tau_i) = i$ and $c(k,i)$ is the signless Stirling number of the first kind.

Special Case 2

Corollary

If X is strongly symmetric, then we have

$$|\overline{X}| = \sum_{i=1}^{k} (-1)^{k-i} c(k,i) |X_i|,$$

where X_i is defined as X_{τ_i} for some $\tau_i \in S_k$ with $l(\tau_i) = i$ and $c(k,i)$ is the signless Stirling number of the first kind.

- The number of terms is k.

Brief Review

$$2^{\binom{k}{2}} \longrightarrow k! \longrightarrow p(k) \longrightarrow k.$$

Proof-0

Lemma (*Möbius* Inversion Formula)

Let $(P, \leq)$ be a finite partially ordered set. Let $f, g : P \to \mathbb{C}$. Then

$$g(x) = \sum_{x \leq y} f(y), \textit{ for all } x \in P$$

if and only if

$$f(x) = \sum_{x \leq y} \mu(x, y) g(y), \textit{ for all } x \in P$$

where $\mu(x, y)$ is the Möbius function defined over the incidence algebra Inc(P).

Proof-1

- Let $[k]$ be the set $\{1, 2, \cdots, k\}$. Let Π_k be the set of set partitions of $[k]$.

Proof-1

- Let $[k]$ be the set $\{1, 2, \cdots, k\}$. Let Π_k be the set of set partitions of $[k]$.
- Define a binary relation "$\leq$" on Π_k as follows: $\tau \leq \delta$ if every block of τ is contained in a block of δ.

Proof-1

- Let $[k]$ be the set $\{1, 2, \cdots, k\}$. Let Π_k be the set of set partitions of $[k]$.
- Define a binary relation " $\leq$ " on Π_k as follows: $\tau \leq \delta$ if every block of τ is contained in a block of δ.
- For instance, $\{1, 2\}\{3, 4\}\{5, 6\} \leq \{1, 2, 3, 4\}\{5, 6\}$ and $\{1, 3\}\{2\}\{4\}\{5\}\{6\} \leq \{1, 2, 3\}\{4\}\{5, 6\}$.

Proof-1

- Let $[k]$ be the set $\{1, 2, \cdots, k\}$. Let Π_k be the set of set partitions of $[k]$.
- Define a binary relation " $\leq$ " on Π_k as follows: $\tau \leq \delta$ if every block of τ is contained in a block of δ.
- For instance, $\{1,2\}\{3,4\}\{5,6\} \leq \{1,2,3,4\}\{5,6\}$ and $\{1,3\}\{2\}\{4\}\{5\}\{6\} \leq \{1,2,3\}\{4\}\{5,6\}$.
- One checks that Π_k is indeed a partially ordered set.

Proof-2

- For a set partition $\tau \in \Pi_k$, define X_τ naturally.

Proof-2

- For a set partition $\tau \in \Pi_k$, define X_τ naturally.
- For any $\tau \in \Pi_k$, define X_τ° to be the set of vectors $x \in X_\tau$ such that there does not exist $\delta \in \Pi_k$ satisfying $\tau < \delta$ and $x \in X_\delta$.

Proof-2

- For a set partition $\tau \in \Pi_k$, define X_τ naturally.
- For any $\tau \in \Pi_k$, define X_τ° to be the set of vectors $x \in X_\tau$ such that there does not exist $\delta \in \Pi_k$ satisfying $\tau < \delta$ and $x \in X_\delta$.

Proof-2

- For a set partition $\tau \in \Pi_k$, define X_τ naturally.
- For any $\tau \in \Pi_k$, define X_τ° to be the set of vectors $x \in X_\tau$ such that there does not exist $\delta \in \Pi_k$ satisfying $\tau < \delta$ and $x \in X_\delta$.
- $$|X_\delta| = \sum_{\delta \leq \tau} |X_\tau^\circ|,$$

Proof-2

- For a set partition $\tau \in \Pi_k$, define X_τ naturally.
- For any $\tau \in \Pi_k$, define X_τ° to be the set of vectors $x \in X_\tau$ such that there does not exist $\delta \in \Pi_k$ satisfying $\tau < \delta$ and $x \in X_\delta$.
- $$|X_\delta| = \sum_{\delta \leq \tau} |X_\tau^\circ|,$$
- and thus by the *Möbius* Inversion Formula we have

$$|X_\delta^\circ| = \sum_{\delta \leq \tau} \mu(\delta, \tau)|X_\tau|.$$

Proof-3

- In particular, let $\delta = 1 = \{1\}\{2\}\cdots\{k\}$, then X_1° is just $\overline{X}$.

Proof-3

- In particular, let $\delta = 1 = \{1\}\{2\}\cdots\{k\}$, then X_1° is just $\overline{X}$.
- Thus we have

$$|\overline{X}| = \sum_{1 \le \tau} \mu(1, \tau)|X_\tau|$$

Proof-3

- In particular, let $\delta = 1 = \{1\}\{2\}\cdots\{k\}$, then X_1° is just $\overline{X}$.
- Thus we have

$$
\begin{aligned}
|\overline{X}| &= \sum_{1 \leq \tau} \mu(1, \tau)|X_\tau| \\
&= \sum_{\tau \in \Pi_k} \mu(1, \tau)|X_\tau|
\end{aligned}
$$

Proof-3

- In particular, let $\delta = 1 = \{1\}\{2\}\cdots\{k\}$, then X_1° is just $\overline{X}$.
- Thus we have

$$
\begin{aligned}
|\overline{X}| &= \sum_{1\leq\tau} \mu(1,\tau)|X_\tau| \\
&= \sum_{\tau\in\Pi_k} \mu(1,\tau)|X_\tau| \\
&= \sum_{\tau\in\Pi_k:(n_1,n_2,\cdots,n_l)} \prod_{i=1}^{l} (-1)^{n_i-1}(n_i-1)!|X_\tau|
\end{aligned}
$$

Proof-3

- In particular, let $\delta = 1 = \{1\}\{2\}\cdots\{k\}$, then X_1° is just $\overline{X}$.
- Thus we have

$$\begin{aligned} |\overline{X}| &= \sum_{1 \leq \tau} \mu(1,\tau)|X_\tau| \\ &= \sum_{\tau \in \Pi_k} \mu(1,\tau)|X_\tau| \\ &= \sum_{\tau \in \Pi_k : (n_1, n_2, \cdots, n_l)} \prod_{i=1}^{l} (-1)^{n_i - 1}(n_i - 1)!|X_\tau| \\ &= \sum_{\tau \in S_k} sign(\tau)|X_\tau|. \end{aligned}$$

Proof-3

- In particular, let $\delta = 1 = \{1\}\{2\}\cdots\{k\}$, then X_1° is just $\overline{X}$.
- Thus we have

$$
\begin{aligned}
|\overline{X}| &= \sum_{1 \leq \tau} \mu(1,\tau)|X_\tau| \\
&= \sum_{\tau \in \Pi_k} \mu(1,\tau)|X_\tau| \\
&= \sum_{\tau \in \Pi_k : (n_1, n_2, \cdots, n_l)} \prod_{i=1}^{l} (-1)^{n_i - 1}(n_i - 1)!|X_\tau| \\
&= \sum_{\tau \in S_k} sign(\tau)|X_\tau|.
\end{aligned}
$$

- The last equality comes from an elementary counting on the number of permutations for a given set partition of $[k]$.

Application on Generators over Finite Fields

Theorem (J. Li and D. Wan, 2009)

Let $A = \mathbb{F}_{q^h}^* = \mathbb{F}_q[\alpha]^*$ and $D = \{\alpha + a | a \in \mathbb{F}_q\}$. Then, for any $\epsilon > 0$, there is a constant $c_\epsilon > 0$ such that if $h < \epsilon k^{1/2}$ and $4\epsilon^2 \ln^2 q < k \leq c_\epsilon q$, we have $N_D(k, b) > 0$ for any $b \in \mathbb{F}_{q^h}^*$. In other words, each element of $\mathbf{F}_{q^h}^*$ can be written to the product of precisely k distinct factors each in $\{\alpha + a, a \in \mathbf{F}_q\}$.

Applications on Counting Rational Points

- Let N be the number of k-subset $S \subseteq \mathbf{F}_q$ satisfying that:

$$\sum_{a \in S} a = b_1,$$

$$\sum_{\{a,b\} \subseteq S} ab = b_2,$$

$$\cdots,$$

$$\sum_{\{a,b,\cdots,c\} \subseteq \in S} ab \cdots c = b_m.$$

Then we have

Applications on Counting Rational Points

- Let N be the number of k-subset $S \subseteq \mathbf{F}_q$ satisfying that:

$$\sum_{a \in S} a = b_1,$$

$$\sum_{\{a,b\} \subseteq S} ab = b_2,$$

$$\cdots,$$

$$\sum_{\{a,b,\cdots,c\} \subseteq \in S} ab \cdots c = b_m.$$

  Then we have

- $$\left| N - \frac{1}{q^m} \binom{q}{k} \right| \le \binom{q/p + m\sqrt{q} + k}{k}.$$

Result on Counting Subsets over Finite Abelian Groups

Theorem (J. Li and D. Wan, 2011)

Suppose we are given the isomorphism $A \cong \mathbb{Z}_{n_1} \times \mathbb{Z}_{n_2} \times \cdots \times \mathbb{Z}_{n_s}$ with $n = |A| = n_1 \cdots n_s$. Given $b \in A$, suppose $(b_1, b_2, \cdots, b_s)$ is the image of b in the isomorphism. Let $N(k, b)$ be the number of k-subsets of A whose elements sum to b. Then we have

$$N(k, b) = \frac{1}{n} \sum_{r|(n,k)} (-1)^{k+\frac{k}{r}} \binom{n/r}{k/r} \Phi(r, b),$$

where $\Phi(r, b) = \sum_{d|r,(n_i,d)|b_i} \mu(r/d) \prod_{i=1}^{s} (n_i, d)$ and μ is the usual Möbius function defined over the integers.

Remark

- In particular, when A is cyclic then

$$\Phi(r,b) = \sum_{d \mid (b,r)} \mu(r/d)d,$$

and the formular for this case was first found by Ramanathan in 1944 using the properties of the Ramanujan's trigonometrical sum.

Remark

- In particular, when A is cyclic then
$$\Phi(r,b)=\sum_{d|(b,r)}\mu(r/d)d,$$
and the formular for this case was first found by Ramanathan in 1944 using the properties of the Ramanujan's trigonometrical sum.
- Interestingly, $\Phi(r,b)$ can be also defined as
$$\Phi(r,b)=\sum_{k,(k,r)=1}e^{2\pi ikb/r}.$$

Remark

- In particular, when A is cyclic then

$$\Phi(r, b) = \sum_{d|(b,r)} \mu(r/d)d,$$

  and the formular for this case was first found by Ramanathan in 1944 using the properties of the Ramanujan's trigonometrical sum.

- Interestingly, $\Phi(r, b)$ can be also defined as

$$\Phi(r, b) = \sum_{k,(k,r)=1} e^{2\pi ikb/r}.$$

- In particular,

$$N(k, 0) = \frac{1}{n} \sum_{r|(n,k)} (-1)^{k+\frac{k}{r}} \phi(r) \binom{n/r}{k/r},$$

  where ϕ is the Euler function.

Corollary

Theorem

Let $N(b)$ be the number of subsets of A sum to b. Then we have

$$N(b) = \frac{1}{n} \sum_{r|n, r \text{ odd}} \Phi(r, b) 2^{n/r}.$$

Corollary

Theorem

Let N(b) be the number of subsets of A sum to b. Then we have

$$N(b) = \frac{1}{n} \sum_{r|n, r \text{ odd}} \Phi(r, b) 2^{n/r}.$$

Furthermore, if A is cyclic and n is odd then we get a classical formula

$$N(0) = \frac{1}{n} \sum_{r|n} \phi(r) 2^{n/r}.$$

Corollary

Theorem

Let $\mathbb{F}_q$ be the finite field of q elements with characteristic p. Let A be any additive subgroup of $\mathbb{F}_q$ and $|A| = n$. For any $b \in A$, let $N(k, b)$ be the number of k-subsets of A whose elements sum to b. Define $v(b) = -1$ if $b \neq 0$, and $v(b) = n - 1$ if $b = 0$. If $p \nmid k$, then

$$N(k, b) = \frac{1}{n}\binom{n}{k}.$$

If $p \mid k$, then

$$N(k, b) = \frac{1}{n}\binom{n}{k} + (-1)^{k+\frac{k}{p}}\frac{v(b)}{n}\binom{n/p}{k/p}.$$

Zhu-Wan's result on Cyclotomic subgroups

- Let $A = \mathbb{F}_q^*$ and D be a multiplicative subgroup of $\mathbb{F}_q^*$ with index m;

Zhu-Wan's result on Cyclotomic subgroups

- Let $A = \mathbb{F}_q^*$ and D be a multiplicative subgroup of $\mathbb{F}_q^*$ with index m;

Theorem (Zhu and Wan, 2011)

Then for $1 \le k \le \frac{q-1}{m}$ *we have*

$$\left| N_D(k,0) - \frac{1}{q}\binom{\frac{q-1}{m}}{k} \right| \le \binom{\sqrt{q} + k + \frac{q}{mp}}{k}.$$

Zhu-Wan's result on Cyclotomic subgroups

- Let $A = \mathbb{F}_q^*$ and D be a multiplicative subgroup of $\mathbb{F}_q^*$ with index m;

Theorem (Zhu and Wan, 2011)

Then for $1 \leq k \leq \frac{q-1}{m}$ *we have*

$$\left| N_D(k,0) - \frac{1}{q}\binom{\frac{q-1}{m}}{k} \right| \leq \binom{\sqrt{q} + k + \frac{q}{mp}}{k}.$$

- Corollary: Let $p > 2$. There is an effectively computable absolute constant 0 < c < 1 such that if $m < c\sqrt{q}$ and $6 \ln q < k \leq \frac{q-1}{2m}$, then $N_D(k,b) > 0$ for all $b \in \mathbb{F}_q$.

Applications in Additive Combinatorics

- We say a subset $D \subseteq A$ is smooth if for any nontrivial additive character χ, $|\sum_{a \in D} \chi(a)| = O(\sqrt{n \log |A|})$.

Applications in Additive Combinatorics

- We say a subset $D \subseteq A$ is smooth if for any nontrivial additive character χ, $|\sum_{a \in D} \chi(a)| = O(\sqrt{n \log |A|})$.

Theorem (Li, 2011)

Let $D \subseteq \mathbb{Z}_p$ and ϵ be a positive constant. If $|D| = \log^{1+\epsilon} p$ and D is smooth, then there is two constants c_1 and c_2 such that when $c_1 \frac{\log p}{\log \log p} \leq k \leq c_2 n$, we have $D^k = \mathbb{Z}_p$.

Thank you very much for your attention!