Submodular Function Minimization under Congruency Constraints

Martin Nägele
ETH Zurich

Benny Sudakov
ETH Zurich

Rico Zenklusen
ETH Zurich

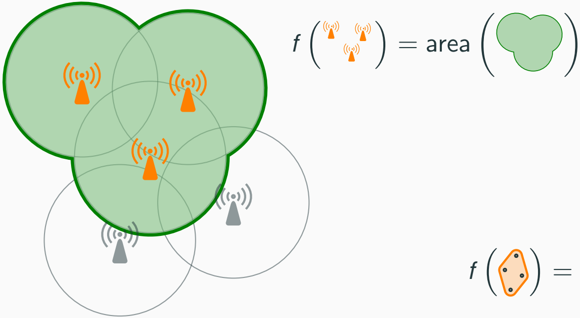
- Submodular function: Set function $f\colon 2^N \to \mathbb{R}$ on finite set N such that

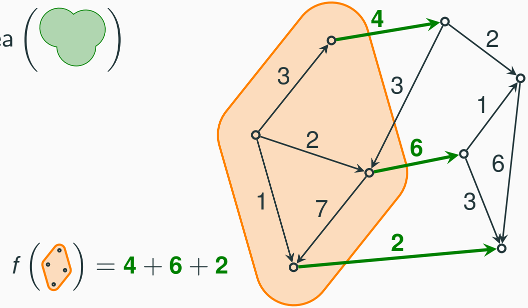
$$\forall A, B \subseteq N: \quad f(A) + f(B) \geqslant f(A \cup B) + f(A \cap B) \ .$$

- Submodular function: Set function $f\colon 2^N \to \mathbb{R}$ on finite set N such that

$$\forall A, B \subseteq N\colon \quad f(A) + f(B) \geqslant f(A \cup B) + f(A \cap B) \ .$$

- Examples: coverage functions, cut functions, rank functions for matroids.





$$\text{Find } S^* \in \operatorname*{argmin}_{S \subseteq N} f(S) \ .$$

$$\text{Find } S^* \in \operatorname*{argmin}_{S \subseteq N} f(S) \ .$$

- History of SFM algorithms:
  - *1981:* Weakly polynomial (ellipsoid-based) [Grötschel, Lovász, Schrijver].
  - *1985:* Combinatorial pseudo-polynomial [Cunningham].
  - *1988:* Strongly polynomial (ellipsoid-based) [Grötschel, Lovász, Schrijver].
  - *1999:* Combinatorial strongly polynomial [Iwata, Fleischer, Fujishige] and [Schrijver].
  - *2009 – :* Speedups [Orlin 2009], [Lee, Sidford, Wong 2015], [Chakraborty, Lee, Sidford, Wong 2017], [Dadush, Végh, Zambelli 2018].

$$\text{Find } S^* \in \operatorname*{argmin}_{S \subseteq N} f(S) \ .$$

- History of SFM algorithms:

  1981: Weakly polynomial (ellipsoid-based) [Grötschel, Lovász, Schrijver].

  1985: Combinatorial pseudo-polynomial [Cunningham].

  1988: Strongly polynomial (ellipsoid-based) [Grötschel, Lovász, Schrijver].

  1999: Combinatorial strongly polynomial [Iwata, Fleischer, Fujishige] and [Schrijver].

  2009 – : Speedups [Orlin 2009], [Lee, Sidford, Wong 2015], [Chakraborty, Lee, Sidford, Wong 2017], [Dadush, Végh, Zambelli 2018].

- Constrained submodular minimization becomes hard quickly.

  With cardinality lower bound: Inapproximable within factor $o\left(\sqrt{|N|/\log|N|}\right)$ [Svitkina, Fleischer 2011].

$$\text{Find } S^* \in \operatorname*{argmin}_{S \subseteq N} f(S) \; .$$

- History of SFM algorithms:
  - *1981:* Weakly polynomial (ellipsoid-based) [Grötschel, Lovász, Schrijver].
  - *1985:* Combinatorial pseudo-polynomial [Cunningham].
  - *1988:* Strongly polynomial (ellipsoid-based) [Grötschel, Lovász, Schrijver].
  - *1999:* Combinatorial strongly polynomial [Iwata, Fleischer, Fujishige] and [Schrijver].
  - *2009 – :* Speedups [Orlin 2009], [Lee, Sidford, Wong 2015], [Chakraborty, Lee, Sidford, Wong 2017], [Dadush, Végh, Zambelli 2018].
- Constrained submodular minimization becomes hard quickly.

With cardinality lower bound: Inapproximable within factor $o\left(\sqrt{|N| / \log |N|}\right)$ [Svitkina, Fleischer 2011].

Under what constraints is efficient submodular function minimization possible?

Constrained submodular minimization: Prior results

- Parity-constrained SFM:

$$\boxed{\text{Find } S^* \in \operatorname*{argmin}_{S \subseteq N,\ |S| \text{ odd}} f(S)\ .}$$

- Parity-constrained SFM:

$$\boxed{\text{Find } S^* \in \operatorname*{argmin}_{S \subseteq N,\ |S| \text{ odd}} f(S)\ .}$$

  - Motivation: Separation over perfect matching polytope.
  - Recent application: Key ingredient for solving bimodular integer programs [Artmann, Weismantel, Zenklusen 2017].

- Parity-constrained SFM:

$$\text{Find } S^* \in \underset{S\subseteq N,\ |S| \text{ odd}}{\operatorname{argmin}} \ f(S)\ .$$

  - Motivation: Separation over perfect matching polytope.
  - Recent application: Key ingredient for solving bimodular integer programs [Artmann, Weismantel, Zenklusen 2017].

- Captured by more general constraint families over which SFM can be done efficiently:
  - *Triple families* [Grötschel, Lovasz, Schrijver 1984].
  - *Parity families* [Goemans, Ramakrishnan 1995].

- Long-standing open problem:

Can p-modular ILPs be solved efficiently?

  - Well-known for unimodular systems.
  - True for bimodular systems [Artmann, Weismantel, Zenklusen 2017].
  - Captures finding minimum cuts of size $\equiv r \pmod{p}$.

- Long-standing open problem:

  Can p-modular ILPs be solved efficiently?

  - Well-known for unimodular systems.
  - True for bimodular systems [Artmann, Weismantel, Zenklusen 2017].
  - Captures finding minimum cuts of size $\equiv r \pmod{p}$.

- Open questions [Geelen, Kapaida 2017]:

t-Set Even-Cut Problem	t-Set Odd-Cut Problem
Let $G = (V, E)$ a graph and $T_1, \ldots, T_t \subseteq V$. Find a non-empty $S \subsetneq V$ s.t. $\lvert S \cap T_i \rvert$ are all even and $\lvert\delta(S)\rvert$ is minimized.	Let $G = (V, E)$ a graph and $T_1, \ldots, T_t \subseteq V$. Find a non-empty $S \subsetneq V$ s.t. $\lvert S \cap T_i \rvert$ are all odd and $\lvert\delta(S)\rvert$ is minimized.

- **Congruency-Constrained Submodular Minimization (CCSM):**

  Let $f\colon 2^N \to \mathbb{Z}$ be submodular, let $m \in \mathbb{Z}_{>0}$, and let $r \in \{0, \ldots, m-1\}$.

$$\begin{aligned} \min\ & f(S) \\ \text{s.t.}\quad & S \subseteq N, \\ & |S| \equiv r \pmod{m}. \end{aligned} \tag{CCSM}$$

Theorem 1: Solving CCSM

For any $m \in \mathbb{Z}_{>0}$ that is a prime power, (CCSM) can be solved in time $|N|^{2m+\mathcal{O}(1)}$.

- **Generalised Congruency-Constrained Submodular Minimization (GCCSM):**

  Let $f\colon 2^N \to \mathbb{Z}$ submodular, $m \in \mathbb{Z}_{>0}$, $k \in \mathbb{Z}_{>0}$, $r_1, \ldots, r_k \in \{0, \ldots, m-1\}$, and $S_1, \ldots, S_k \subseteq N$.

$$\begin{aligned} \min\ & f(S) \\ \text{s.t.}\quad & S \subseteq N, \\ & |S \cap S_i| \equiv r_i \pmod{m} \quad \forall i \in [k]. \end{aligned} \tag{GCCSM}$$

Theorem 2: Solving GCCSM

For any $m \in \mathbb{Z}_{>0}$ that is a prime power, (GCCSM) can be solved in time $|N|^{2km+\mathcal{O}(1)}$.

- **Generalised Congruency-Constrained Submodular Minimization (GCCSM):**

  Let $f\colon 2^N \to \mathbb{Z}$ submodular, $m \in \mathbb{Z}_{>0}$, $k \in \mathbb{Z}_{>0}$, $r_1, \dots, r_k \in \{0, \dots, m-1\}$, and $S_1, \dots, S_k \subseteq N$.

$$\begin{aligned} \min\ & f(S) \\ \text{s.t.}\quad & S \subseteq N, \\ & |S \cap S_i| \equiv r_i \pmod{m} \quad \forall i \in [k]. \end{aligned} \tag{GCCSM}$$

Theorem 2: Solving GCCSM

For any $m \in \mathbb{Z}_{>0}$ that is a prime power, (GCCSM) can be solved in time $|N|^{2km+\mathcal{O}(1)}$.

- Captures both the *t*-Set Even-Cut Problem and the *t*-Set Odd-Cut Problem.

- Focus on **CCSM**: Minimize f over sets $S \subseteq N$ with $|S| \equiv r \pmod{m}$.

- Focus on **CCSM**: Minimize f over sets $S \subseteq N$ with $|S| \equiv r \pmod{m}$.

$\mathrm{Enum}(d)$: Enumeration algorithm of depth d for CCSM

1. For all disjoint $A, B \subseteq N$ with $|A|, |B| \leqslant d$, find a minimal minimizer of f over

$$\mathcal{L}_{AB} := \{S \subseteq N \mid A \subseteq S \subseteq N \setminus B\} \ .$$

   Let $\mathcal{S}$ contain one minimal minimizer for each pair (A, B).

2. Among all $S \in \mathcal{S}$ with $|S| \equiv r \pmod{m}$, return best one.

- Focus on **CCSM**: Minimize f over sets $S \subseteq N$ with $|S| \equiv r \pmod m$.

$\mathrm{Enum}(d)$: Enumeration algorithm of depth d for CCSM

1. For all disjoint $A, B \subseteq N$ with $|A|, |B| \leqslant d$, find a minimal minimizer of f over

$$\mathcal{L}_{AB} := \{S \subseteq N \mid A \subseteq S \subseteq N \setminus B\} \ .$$

   Let $\mathcal{S}$ contain one minimal minimizer for each pair (A, B).

2. Among all $S \in \mathcal{S}$ with $|S| \equiv r \pmod m$, return best one.

- $\mathrm{Enum}(d)$ is extension of algorithm in [Goemans, Ramakrishnan 1995].

- Reduction to a purely combinatorial question about set systems.

- Reduction to a purely combinatorial question about set systems.

Definition: (m, d)-system

For a finite set N, a family $\mathcal{H} \subseteq 2^N$ is called (m, d)-system on N if

(i) $\mathcal{H}$ is closed under intersection,

(ii) $|H| \not\equiv |N| \pmod{m}$ $\forall H \in \mathcal{H}$, and

(iii) for any $S \subseteq N$ with $|S| \leq d$, there is a set $H \in \mathcal{H}$ with $S \subseteq H$.

- Reduction to a purely combinatorial question about set systems.

Definition: (m,d)-system

For a finite set N, a family $\mathcal{H} \subseteq 2^N$ is called (m,d)-system on N if

(i) $\mathcal{H}$ is closed under intersection,

(ii) $|H| \not\equiv |N| \pmod{m}$ $\forall H \in \mathcal{H}$, and

(iii) for any $S \subseteq N$ with $|S| \leq d$, there is a set $H \in \mathcal{H}$ with $S \subseteq H$.

Theorem 3: Reduction

If no (m,d)-system exists, then $\mathrm{Enum}(d)$ solves any CCSM problem with modulus m.

- Reduction to a purely combinatorial question about set systems.

Definition: (m, d)-system

For a finite set N, a family $\mathcal{H} \subseteq 2^N$ is called (m, d)-system on N if

(i) $\mathcal{H}$ is closed under intersection,

(ii) $|H| \not\equiv |N| \pmod{m}$ $\forall H \in \mathcal{H}$, and

(iii) for any $S \subseteq N$ with $|S| \leq d$, there is a set $H \in \mathcal{H}$ with $S \subseteq H$.

Theorem 3: Reduction

If no (m, d)-system exists, then $\mathrm{Enum}(d)$ solves any CCSM problem with modulus m.

Theorem 4: Inexistence of systems

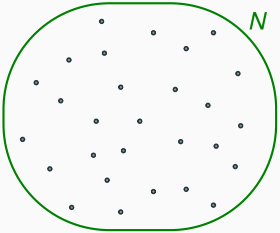
For $m \in \mathbb{Z}_{>0}$ being a prime power, there is no $(m, m-1)$-system.

Assumptions:

- No ties, i.e., $f(S_1) \neq f(S_2)$ for all $S_1 \neq S_2$.

Assumptions:

- No ties, i.e., $f(S_1) \neq f(S_2)$ for all $S_1 \neq S_2$.
- N is an optimizer of the problem.

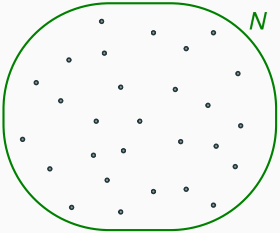


$$|N| \equiv r \pmod{m}$$

$$f(N) = \min_{\substack{S \subseteq N, \\ |S| \equiv r \pmod{m}}} f(S)$$

Assumptions:

- No ties, i.e., $f(S_1) \neq f(S_2)$ for all $S_1 \neq S_2$.
- N is an optimizer of the problem.
- $\mathrm{Enum}(d)$ does not return N.



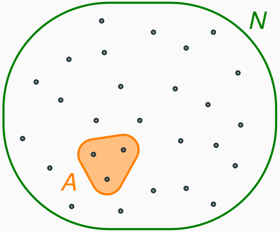
$$|N| \equiv r \pmod{m}$$

$$f(N) = \min_{\substack{S \subseteq N,\\ |S| \equiv r \pmod{m}}} f(S)$$

Reduction in a much simplified case

Assumptions:

- No ties, i.e., $f(S_1) \neq f(S_2)$ for all $S_1 \neq S_2$.
- N is an optimizer of the problem.
- $\mathrm{Enum}(d)$ does not return N.



$$|N| \equiv r \pmod{m}$$

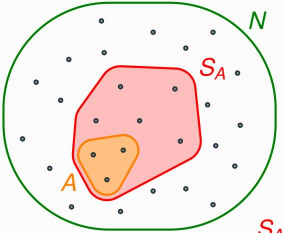
$$f(N) = \min_{\substack{S \subseteq N, \\ |S| \equiv r \pmod{m}}} f(S)$$

$$|A| \leqslant d$$

Reduction in a much simplified case

Assumptions:

- No ties, i.e., $f(S_1) \neq f(S_2)$ for all $S_1 \neq S_2$.
- N is an optimizer of the problem.
- $\mathrm{Enum}(d)$ does not return N.



$$|N| \equiv r \pmod{m}$$

$$f(N) = \min_{\substack{S \subseteq N, \\ |S| \equiv r \pmod{m}}} f(S)$$

$$|A| \leqslant d$$

$$S_A : \quad A \subseteq S_A \subsetneq N,$$

$$f(S_A) = \min_{S:\, A \subseteq S \subseteq N} f(S)$$

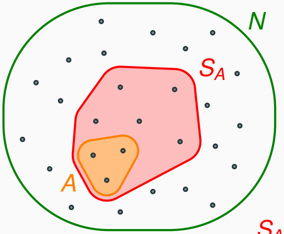
Assumptions:

- No ties, i.e., $f(S_1) \neq f(S_2)$ for all $S_1 \neq S_2$.
- N is an optimizer of the problem.
- $\mathrm{Enum}(d)$ does not return N.

Claim

The following family $\mathcal{H}$ is an (m, d)-system:

$$\mathcal{H} := \left\{ \bigcap_{i=1}^{k} S_{A_i} \;\middle|\; k \geqslant 1, A_i \subseteq N, |A_i| \leqslant d \right\} .$$



$|N| \equiv r \pmod{m}$

$$f(N) = \min_{\substack{S \subseteq N, \\ |S| \equiv r \pmod{m}}} f(S)$$

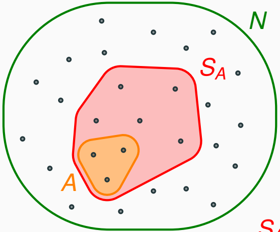
$|A| \leqslant d$

S_A : $A \subseteq S_A \subsetneq N$,

$$f(S_A) = \min_{S:\, A \subseteq S \subseteq N} f(S)$$

Assumptions:

- No ties, i.e., $f(S_1) \neq f(S_2)$ for all $S_1 \neq S_2$.
- N is an optimizer of the problem.
- $\mathrm{Enum}(d)$ does not return N.



$$|N| \equiv r \pmod{m}$$

$$f(N) = \min_{\substack{S \subseteq N, \\ |S| \equiv r \pmod{m}}} f(S)$$

$$|A| \leqslant d$$

$$S_A : \quad A \subseteq S_A \subsetneq N,$$

$$f(S_A) = \min_{S:\, A \subseteq S \subseteq N} f(S)$$

Claim

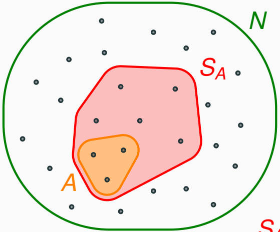
The following family $\mathcal{H}$ is an (m, d)-system:

$$\mathcal{H} := \left\{ \bigcap_{i=1}^{k} S_{A_i} \;\middle|\; k \geqslant 1, A_i \subseteq N, |A_i| \leqslant d \right\} .$$

Proof. (i) closed under intersections (ii) $|H| \not\equiv |N| \pmod{m}$ $\forall H \in \mathcal{H}$ (iii) covering property

Assumptions:

- No ties, i.e., $f(S_1) \neq f(S_2)$ for all $S_1 \neq S_2$.
- N is an optimizer of the problem.
- $\mathrm{Enum}(d)$ does not return N.



$$|N| \equiv r \pmod{m}$$

$$f(N) = \min_{\substack{S \subseteq N, \\ |S| \equiv r \pmod{m}}} f(S)$$

$$|A| \leqslant d$$

$$S_A: \quad A \subseteq S_A \subsetneq N,$$

$$f(S_A) = \min_{S:\, A \subseteq S \subseteq N} f(S)$$

Claim

The following family $\mathcal{H}$ is an (m, d)-system:

$$\mathcal{H} := \left\{ \bigcap_{i=1}^{k} S_{A_i} \;\middle|\; k \geqslant 1, A_i \subseteq N, |A_i| \leqslant d \right\} .$$

Proof. (i) closed under intersections (ii) $|H| \not\equiv |N| \pmod{m}\ \forall H \in \mathcal{H}$ (iii) covering property

ad (ii):

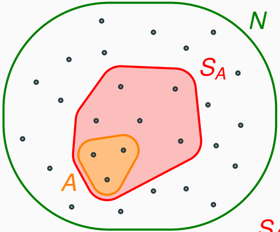
$$f(N) > f(S_{A_1})$$

$$\Longrightarrow \quad |S_{A_1}| \not\equiv |N| \pmod{m}$$

Reduction in a much simplified case

Assumptions:

- No ties, i.e., $f(S_1) \neq f(S_2)$ for all $S_1 \neq S_2$.
- N is an optimizer of the problem.
- $\mathrm{Enum}(d)$ does not return N.



$|N| \equiv r \pmod{m}$

$f(N) = \min\limits_{\substack{S \subseteq N, \\ |S| \equiv r \pmod{m}}} f(S)$

$|A| \leqslant d$

$S_A: \quad A \subseteq S_A \subsetneq N,$

$f(S_A) = \min\limits_{S:\, A \subseteq S \subseteq N} f(S)$

Claim

The following family $\mathcal{H}$ is an (m, d)-system:

$$\mathcal{H} := \left\{ \bigcap_{i=1}^{k} S_{A_i} \;\middle|\; k \geqslant 1, A_i \subseteq N, |A_i| \leqslant d \right\} .$$

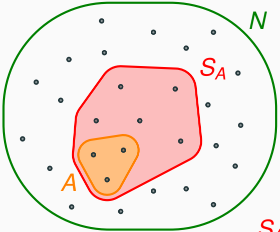
Proof. (i) closed under intersections (ii) $|H| \not\equiv |N| \pmod{m}$ $\forall H \in \mathcal{H}$ (iii) covering property

ad (ii): $f(N) > f(S_{A_1})$ $\quad f(S_{A_1}) + f(S_{A_2}) \geqslant f(S_{A_1} \cup S_{A_2}) + f(S_{A_1} \cap S_{A_2})$

$\Longrightarrow \quad |S_{A_1}| \not\equiv |N| \pmod{m}$

Assumptions:

- No ties, i.e., $f(S_1) \neq f(S_2)$ for all $S_1 \neq S_2$.
- N is an optimizer of the problem.
- $\mathrm{Enum}(d)$ does not return N.



$$|N| \equiv r \pmod{m}$$

$$f(N) = \min_{\substack{S \subseteq N, \\ |S| \equiv r \pmod{m}}} f(S)$$

$$|A| \leqslant d$$

$$S_A: \quad A \subseteq S_A \subsetneq N,$$

$$f(S_A) = \min_{S:\, A \subseteq S \subsetneq N} f(S)$$

Claim

The following family $\mathcal{H}$ is an (m, d)-system:

$$\mathcal{H} := \left\{ \bigcap_{i=1}^{k} S_{A_i} \;\middle|\; k \geqslant 1, A_i \subseteq N, |A_i| \leqslant d \right\} .$$

Proof. (i) closed under intersections (ii) $|H| \not\equiv |N| \pmod{m}$ $\forall H \in \mathcal{H}$ (iii) covering property

ad (ii):

$$f(N) > f(S_{A_1})$$

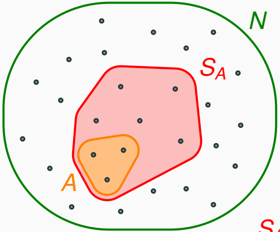
$$\implies |S_{A_1}| \not\equiv |N| \pmod{m}$$

$$f(S_{A_1}) + \underbrace{f(S_{A_2})}_{< f(N)} \geqslant \underbrace{f(S_{A_1} \cup S_{A_2})}_{\geqslant f(S_{A_1})} + f(S_{A_1} \cap S_{A_2})$$

Reduction in a much simplified case

Assumptions:

- No ties, i.e., $f(S_1) \neq f(S_2)$ for all $S_1 \neq S_2$.
- N is an optimizer of the problem.
- $\mathrm{Enum}(d)$ does not return N.



$$|N| \equiv r \pmod{m}$$

$$f(N) = \min_{\substack{S \subseteq N, \\ |S| \equiv r \pmod{m}}} f(S)$$

$$|A| \leqslant d$$

$$S_A : \quad A \subseteq S_A \subsetneq N,$$

$$f(S_A) = \min_{S:\, A \subseteq S \subsetneq N} f(S)$$

Claim

The following family $\mathcal{H}$ is an (m, d)-system:

$$\mathcal{H} := \left\{ \bigcap_{i=1}^{k} S_{A_i} \;\middle|\; k \geqslant 1, A_i \subseteq N, |A_i| \leqslant d \right\} .$$

Proof. (i) closed under intersections (ii) $|H| \not\equiv |N| \pmod{m}\ \forall H \in \mathcal{H}$ (iii) covering property

ad (ii):

$$f(N) > f(S_{A_1})$$

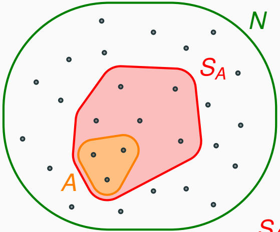
$$\implies |S_{A_1}| \not\equiv |N| \pmod{m}$$

$$f(S_{A_1}) + \underbrace{f(S_{A_2})}_{<f(N)} \geqslant \underbrace{f(S_{A_1} \cup S_{A_2})}_{\geqslant f(S_{A_1})} + f(S_{A_1} \cap S_{A_2})$$

$$\implies f(N) > f(S_{A_1} \cap S_{A_2})$$

Assumptions:

- No ties, i.e., $f(S_1) \neq f(S_2)$ for all $S_1 \neq S_2$.
- N is an optimizer of the problem.
- $\mathrm{Enum}(d)$ does not return N.



$$|N| \equiv r \pmod m$$

$$f(N) = \min_{\substack{S \subseteq N, \\ |S| \equiv r \pmod m}} f(S)$$

$$|A| \leqslant d$$

$$S_A : \quad A \subseteq S_A \subsetneq N,$$

$$f(S_A) = \min_{S:\, A \subseteq S \subseteq N} f(S)$$

Claim

The following family $\mathcal{H}$ is an (m, d)-system:

$$\mathcal{H} := \left\{ \bigcap_{i=1}^{k} S_{A_i} \;\middle|\; k \geqslant 1, A_i \subseteq N, |A_i| \leqslant d \right\} .$$

Proof. (i) closed under intersections (ii) $|H| \not\equiv |N| \pmod m \ \forall H \in \mathcal{H}$ (iii) covering property

ad (ii):

$$f(N) > f(S_{A_1})$$

$$\implies |S_{A_1}| \not\equiv |N| \pmod m$$

$$f(S_{A_1}) + \underbrace{f(S_{A_2})}_{<f(N)} \geqslant \underbrace{f(S_{A_1} \cup S_{A_2})}_{\geqslant f(S_{A_1})} + f(S_{A_1} \cap S_{A_2})$$

$$\implies f(N) > f(S_{A_1} \cap S_{A_2}) \qquad \square$$

First steps: No $(2, 1)$-system exists

Properties of a $(2, 1)$-system $\mathcal{H}$

- Closed under intersections.
- $|H| \not\equiv |N| \pmod 2$ for all $H \in \mathcal{H}$.
- Any single element is covered by a set in $\mathcal{H}$.

Step 1: We can assume $|N| \equiv 1 \pmod 2$.

- By adding a new element to all sets.
- Implies $|H| \equiv 0 \pmod 2$ for all $H \in \mathcal{H}$.

Properties of a $(2,1)$-system $\mathcal{H}$

- Closed under intersections.
- $|H| \not\equiv |N| \pmod 2$ for all $H \in \mathcal{H}$.
- Any single element is covered by a set in $\mathcal{H}$.

First steps: No $(2, 1)$-system exists

Step 1: We can assume $|N| \equiv 1 \pmod 2$.

- By adding a new element to all sets.
- Implies $|H| \equiv 0 \pmod 2$ for all $H \in \mathcal{H}$.

Properties of a $(2, 1)$-system $\mathcal{H}$

- Closed under intersections.
- $|H| \not\equiv |N| \pmod 2$ for all $H \in \mathcal{H}$.
- Any single element is covered by a set in $\mathcal{H}$.

Step 2: Contradiction by inclusion-exclusion principle:

$$|N| \underset{\text{covering property}}{=} \left| \bigcup_{H \in \mathcal{H}} H \right| \overset{\text{inclusion-exclusion}}{=} \sum_{\ell=1}^{|\mathcal{H}|} (-1)^{\ell+1} \sum_{\substack{H_1, \ldots, H_\ell \in \mathcal{H}, \\ \forall i \neq j:\ H_i \neq H_j}} \left| \bigcap_{i=1}^{\ell} H_i \right| \underset{\text{Step 1}}{\equiv} 0 \pmod 2 .$$

Proof plan to show that no $(p, p-1)$-system exists

Properties of an (m, d)-system $\mathcal{H}$

- Closed under intersections.
- $|H| \not\equiv |N| \pmod{m}$ for all $H \in \mathcal{H}$.
- Any d elements are covered by a set in $\mathcal{H}$.

Proof plan to show that no $(p, p-1)$-system exists

Problem:

- $H \in \mathcal{H}$ can have different cardinalities $\bmod p$.

Properties of an (m, d)-system $\mathcal{H}$

- Closed under intersections.
- $|H| \not\equiv |N| \pmod{m}$ for all $H \in \mathcal{H}$.
- Any d elements are covered by a set in $\mathcal{H}$.

Problem:

- $H \in \mathcal{H}$ can have different cardinalities mod p.

Lemma

If there exists a $(p, p-1)$-system, then there exists a $(p, 1)$-system such that

$$|H| \equiv 0 \pmod{p} \quad \forall H \in \mathcal{H} \quad .$$

Properties of an (m, d)-system $\mathcal{H}$

- Closed under intersections.
- $|H| \not\equiv |N| \pmod{m}$ for all $H \in \mathcal{H}$.
- Any d elements are covered by a set in $\mathcal{H}$.

Proof plan to show that no $(p, p-1)$-system exists

Problem:

- $H \in \mathcal{H}$ can have different cardinalities mod p.

Lemma

If there exists a $(p, p-1)$-system, then there exists a $(p, 1)$-system such that

$$|H| \equiv 0 \pmod{p} \quad \forall H \in \mathcal{H} \ .$$

Properties of an (m, d)-system $\mathcal{H}$

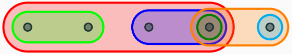
- Closed under intersections.
- $|H| \not\equiv |N| \pmod{m}$ for all $H \in \mathcal{H}$.
- Any d elements are covered by a set in $\mathcal{H}$.

- Exploit inclusion-exclusion again for contradiction:

$$|N| = \left| \bigcup_{H \in \mathcal{H}} H \right| = \sum_{\ell=1}^{|\mathcal{H}|} (-1)^{\ell+1} \sum_{\substack{H_1, \ldots, H_\ell \in \mathcal{H}, \\ \forall i \neq j:\ H_i \neq H_j}} \left| \bigcap_{i=1}^{\ell} H_i \right| \equiv 0 \pmod{p} \ .$$

Step 1: Assume $(p, p-1)$-system $\mathcal{H}$ with $|N| \equiv 0 \pmod{p}$.

- $|H| \not\equiv 0 \pmod{p}$ for all $H \in \mathcal{H}$.

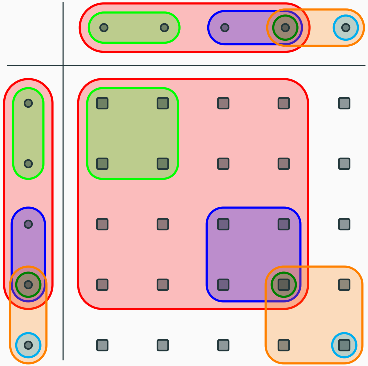


Step 1: Assume $(p, p-1)$-system $\mathcal{H}$ with $|N| \equiv 0 \pmod{p}$.

- $|H| \not\equiv 0 \pmod{p}$ for all $H \in \mathcal{H}$.

Step 2: Transform sets to $(p-1)$-fold cartesian product

- Ground set cardinality: $|N|^{p-1} \equiv 0 \pmod{p}$.
- Set cardinalities: $|H|^{p-1} \equiv 1 \pmod{p}$.
  (Fermat's Little Theorem)
- Obtain $(p, 1)$-system.



Example: 2-fold product for $p = 3$

Step 1: Assume $(p, p-1)$-system $\mathcal{H}$ with $|N| \equiv 0 \pmod p$.

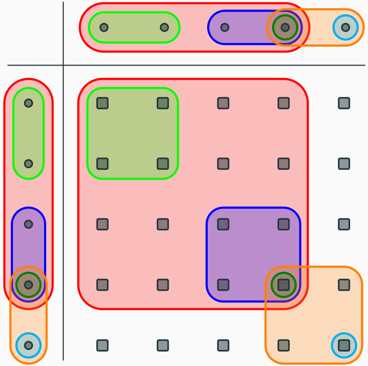
- $|H| \not\equiv 0 \pmod p$ for all $H \in \mathcal{H}$.

Step 2: Transform sets to $(p-1)$-fold cartesian product

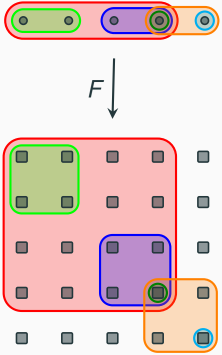
- Ground set cardinality: $|N|^{p-1} \equiv 0 \pmod p$.
- Set cardinalities: $|H|^{p-1} \equiv 1 \pmod p$.
  (Fermat's Little Theorem)
- Obtain $(p, 1)$-system.

Step 3: Shift to obtain $|H| \equiv 0 \pmod p$ for all $H \in \mathcal{H}$.

- By adding $p-1$ elements.



Example: 2-fold product for $p = 3$



- Key ingredient: Set system transformation function F.
- Crucial properties:
  - Cardinality transformation:
  $$|F(S)| \equiv \begin{cases} 0 \pmod{m} & \text{if } |S| \equiv 0 \pmod{m}, \\ 1 \pmod{m} & \text{if } |S| \not\equiv 0 \pmod{m}. \end{cases}$$
  - Preserving intersections:
  $$F(S) \cap F(T) = F(S \cap T).$$
  - Preserving coverage.
- Feasible functions:

  polynomial: $|F(S)| = |S|^k$, *binomial:* $|F(S)| = \binom{|S|}{k}$, *conic combinations thereof*
- Function used for moduli m that are prime powers:
$$|F(S)| = \sum_{\substack{1 \leq k < m, \\ k \text{ odd}}} \binom{|S|}{k} + (p-1) \cdot \sum_{\substack{1 \leq k < m, \\ k \text{ even}}} \binom{|S|}{k} .$$

- Main results: Polynomial-time algorithms for

CCSM

$$\begin{aligned} &\min f(S) \\ \text{s.t.} \quad & S \subseteq N, \\ & |S| \equiv r \pmod{m}. \end{aligned}$$

and

GCCSM

$$\begin{aligned} &\min f(S) \\ \text{s.t.} \quad & S \subseteq N, \\ & |S \cap S_i| \equiv r_i \pmod{m} \ \ \forall i \in [k]. \end{aligned}$$

for constant prime powers m and constant k.

- Main results: Polynomial-time algorithms for

CCSM

$$\begin{aligned} \min\ & f(S) \\ \text{s.t.}\ & S \subseteq N, \\ & |S| \equiv r \pmod{m}. \end{aligned}$$

and

GCCSM

$$\begin{aligned} \min\ & f(S) \\ \text{s.t.}\ & S \subseteq N, \\ & |S \cap S_i| \equiv r_i \pmod{m} \quad \forall i \in [k]. \end{aligned}$$

for constant prime powers m and constant k.

Extension to any $m = O(1)$?

- Main results: Polynomial-time algorithms for

CCSM

$$\begin{aligned} &\min f(S) \\ \text{s.t.}\quad & S \subseteq N, \\ & |S| \equiv r \pmod{m}. \end{aligned}$$

and

GCCSM

$$\begin{aligned} &\min f(S) \\ \text{s.t.}\quad & S \subseteq N, \\ & |S \cap S_i| \equiv r_i \pmod{m} \;\; \forall i \in [k]. \end{aligned}$$

for constant prime powers m and constant k.

Extension to any $m = O(1)$?

- Barrier: $(m, m-1)$-systems do exist for composite m [Gopi 2017].