Uniform Splitting Families

Gabriel Currier and Colin Okasaki

July 31, 2015

Presentation Outline

The Discrete Log Problem

Problem: Let p be a prime. Let a be a primitive root of the multiplicative group $\mathbb{Z}_p^*$ and b an element of $\mathbb{Z}_p^*$. Then the **discrete log problem** is the problem of finding the exponent x so that $a^x = b$.

The Discrete Log Problem

Problem: Let p be a prime. Let a be a primitive root of the multiplicative group $\mathbb{Z}_p^*$ and b an element of $\mathbb{Z}_p^*$. Then the **discrete log problem** is the problem of finding the exponent x so that $a^x = b$.

In general this is thought to be a hard problem but in some special circumstances clever algorithms can make it much easier.

The Low Hamming Weight Discrete Log Problem

Consider the following simplification to the discrete log problem. All else is equivalent, but now it is known that the exponent x has exactly t ones in its binary representation. Is this now a tractable problem?

The Low Hamming Weight Discrete Log Problem

Consider the following simplification to the discrete log problem. All else is equivalent, but now it is known that the exponent x has exactly t ones in its binary representation. Is this now a tractable problem?

As it turns out the answer is yes, and the mathematical objects we have been studying provide a (relatively) efficient solution in $O(m\binom{m/2}{t/2})$ where m is the number of digits in the binary representation of p.

Presentation Outline

Formal Definition

Definition

Let m and t be fixed integers with $0 < t \leq m$. Let X be a set of size m. Let a subset of X be a **block**. A family $\mathcal{F}$ is a set of blocks, and is called an $(\mathbf{m}, \mathbf{t})$-**splitting family** if for all sets $Y \subseteq X$ such that $|Y| = t$, there exists a block $b \in \mathcal{F}$ so that $|b \cap Y| = \lfloor t/2 \rfloor$. We call $\mathcal{F}$ **uniform** if all blocks have size $\lfloor m/2 \rfloor$.

Examples

- An (8,2)-uniform splitting family

$$\mathcal{F} = \{\{1,2,3,4\},\{1,2,5,6\},\{1,3,5,7\}\}$$

Examples

- An (8,2)-uniform splitting family

$$\mathcal{F} = \{\{1,2,3,4\},\{1,2,5,6\},\{1,3,5,7\}\}$$

X	1	2	3	4	5	6	7	8
b_1	1	2	3	4				
b_2	1	2			5	6		
b_3	1		3		5		7	

Examples

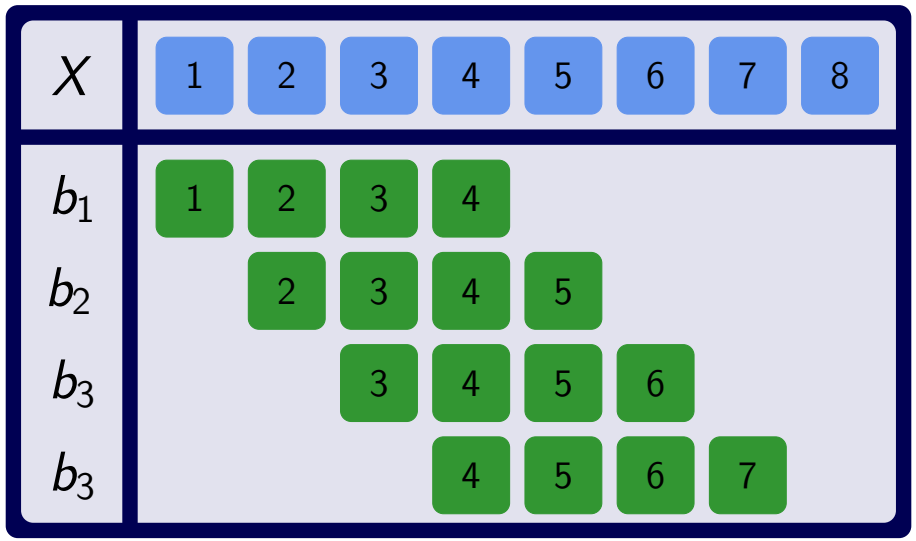
- An (8,4)-uniform splitting family

$$\mathcal{F} = \{\{1,2,3,4\},\{2,3,4,5\},\{3,4,5,6\},\{4,5,6,7\}\}$$

Examples

- An (8,4)-uniform splitting family

$$\mathcal{F} = \{\{1,2,3,4\},\{2,3,4,5\},\{3,4,5,6\},\{4,5,6,7\}\}$$



Examples

- An (8,4)-uniform splitting family

$$\mathcal{F} = \{\{1,2,3,4\},\{2,3,4,5\},\{3,4,5,6\},\{4,5,6,7\}\}$$

$$\begin{bmatrix} 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 1 & 1 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 & 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 & 0 \end{bmatrix}$$

Minimality

Now that we understand what splitting families are we can begin to delve into our research. We are interested in two related types of splitting families: minimum-sized and minimal.

Minimality

Now that we understand what splitting families are we can begin to delve into our research. We are interested in two related types of splitting families: minimum-sized and minimal.

Definition

Let $\mathcal{F}$ be a splitting family. Then, $\mathcal{F}$ is said to be **minimum-sized** if there does not exist a splitting family of smaller size.

Minimality

Now that we understand what splitting families are we can begin to delve into our research. We are interested in two related types of splitting families: minimum-sized and minimal.

Definition

Let $\mathcal{F}$ be a splitting family. Then, $\mathcal{F}$ is said to be **minimum-sized** if there does not exist a splitting family of smaller size.

Definition

Let $\mathcal{F}$ be a splitting family. Then, $\mathcal{F}$ is said to be **minimal** if, for all $b \in \mathcal{F}$, $\mathcal{F} \setminus b$ is not a splitting family.

Minimality

Now that we understand what splitting families are we can begin to delve into our research. We are interested in two related types of splitting families: minimum-sized and minimal.

Definition

Let $\mathcal{F}$ be a splitting family. Then, $\mathcal{F}$ is said to be **minimum-sized** if there does not exist a splitting family of smaller size.

Definition

Let $\mathcal{F}$ be a splitting family. Then, $\mathcal{F}$ is said to be **minimal** if, for all $b \in \mathcal{F}$, $\mathcal{F} \setminus b$ is not a splitting family.

Note, in particular, that all minimum-sized splitting families are also minimal.

Presentation Outline

$(m, 2)$-uniform splitting families

We spent the first half of the summer focusing largely on $(m, 2)$ uniform splitting families, concluding with the following theorem

Theorem

Let $\mathcal{F}$ be a minimal $(m, 2)$ uniform splitting family with $m \geq 6$. Then

$$\lceil \log_2(m) \rceil \leq |\mathcal{F}| \leq m - 3.$$

Uniform splitting families for larger t

Results for $t > 2$ are remarkably harder to come by, but after some work we were able to prove the following upper bound on minimum-sized families using methods presented in [2].

Theorem

Let m and t be even. Let $\mathcal{F}$ be a minimum-sized (m, t) uniform splitting family. Then

$$|\mathcal{F}| \leq \frac{t \log_2(m)}{-\log_2\left(1 - \binom{t}{t/2}\left(\frac{1}{2}\right)^t\right)}.$$

An analogous result holds for m and/or t odd.

A comparison

Below is a comparison of this log bound with the currently best known bounds on maximum size.

m	t	Log bound	Best known [2]
8	4	18	3
10	4	20	5
12	4	22	6
14	4	23	7
16	4	24	6
18	4	25	9
20	4	26	8
22	4	27	11
24	4	28	9
26	4	28	13
38	4	29	14
30	4	29	12

Uniform splitting families for larger t

Bounds on minimal splitting families turned out to be even trickier but we were ultimately able to prove the following upper bound.

Theorem

Let m and t be even. Let $\mathcal{F}$ be a minimal (m, t) uniform splitting family. Then

$$|\mathcal{F}| \leq \frac{2}{3}\binom{m}{t}.$$

Witnesses

To understand this proof, we need the following definition

Witnesses

To understand this proof, we need the following definition

Definition

Let $\mathcal{F}$ be a splitting family, and let Y be a t-set that is split by exactly one block $b \in \mathcal{F}$. Then, we say that Y is a witness for b, and for our splitting family $\mathcal{F}$.

Constructions for $(m, m/2)$

Our constructions have come somewhat short of our bounds on maximum size.

Constructions for $(m, m/2)$

Our constructions have come somewhat short of our bounds on maximum size.

Theorem

For all m divisible by 4, there exists a $(m, m/2)$ splitting family of size

$m/2 \binom{}{m/4.}$.

Constructions for $(m, m/2)$

Our constructions have come somewhat short of our bounds on maximum size.

Theorem

For all m divisible by 4, there exists a $(m, m/2)$ splitting family of size

$m/2 \binom{}{m/4.}$.

What do these look like?

Constructions for $(m, m/2)$

Construction is quite simple. For $(8, 4)$:

Constructions for $(m, m/2)$

Construction is quite simple. For $(8, 4)$:

$$\left[\begin{array}{cc|cccc|cc} 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 \\ 1 & 1 & 1 & 0 & 1 & 0 & 0 & 0 \\ 1 & 1 & 1 & 0 & 0 & 1 & 0 & 0 \\ 1 & 1 & 0 & 1 & 1 & 0 & 0 & 0 \\ 1 & 1 & 0 & 1 & 0 & 1 & 0 & 0 \\ 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 \end{array}\right]$$

Is this the best?

For $m = 4$ and 8, this previous construction is in fact the largest possible

Is this the best?

For $m = 4$ and 8, this previous construction is in fact the largest possible

This is the largest construction we've come up with for any t, indicating that it is probably the upper rather than lower bounds that needs improvement.

References

[1] D. R. Stinson. Some baby-step giant-step algorithms for the low Hamming weight discrete logarithm problem. *Math. Comp.*, 71(237):379-391 (electronic), 2002.

[2] A. C.H. Ling, P. C. Li, G. H. J. van Rees. Splitting systems and separating systems. *Discrete Math* 279 (2004) 355-368,

Acknowledgements

- NSF grant DMS-1359425
- Boise State University
- Our mentors Liljana Babinkostova and Marion Scheepers

Questions?