Practical Numbers and Simple BIBDs

Hsin-Min Sun (孫新民)
Department of Applied Mathematics,
National University of Tainan, Taiwan

2019圖論與組合數學國際研討會
Aug 18-23, 2019

Abstract

A practical number is a positive integer m such that every number less than m can be represented as a sum of distinct divisors of m. We apply the properties of practical numbers in the existence theorem for simple BIBDs. Let q be a power of an odd prime p and $3 \leq k \leq q-3$ with $p \nmid k$. We show that the necessary conditions

(1) $\lambda(q-1) \equiv 0 \mod (k-1)$,

(2) $\lambda q(q-1) \equiv 0 \mod k(k-1)$, and

(3) $\lambda \leq \binom{q-2}{k-2}$

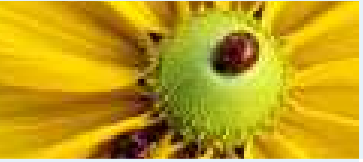
are also sufficient for the existence of a simple (q, k, λ) BIBD when certain conditions regarding practical numbers are satisfied.

Simple BIBDs

BIBDs (Balanced Incomplete Block Designs)

- $v > k \geq 2$
- V: a finite set of symbols, $v = |V|$
- $\mathcal{B}$: a collection of k-subsets (*blocks*) of V
- $(V, \mathcal{B})$ is a (v, k, λ) *BIBD*: every pair of distinct symbols appears in exactly λ blocks

- every symbol appears in exactly r blocks, where $r = \lambda(v-1)/(k-1)$
- $|\mathcal{B}| = b = vr/k$
- *simple* design: no repeated blocks



λ_{min}

Necessary conditions for the existence of a (v, k, λ) BIBD:

(1) $\lambda(v-1) \equiv 0 \mod (k-1)$

(2) $\lambda v(v-1) \equiv 0 \mod k(k-1)$

- λ_{min}: the smallest positive integer that satisfies the necessary conditions
- λ_{min} divides λ whenever a (v, k, λ) BIBD exists
- $\lambda_{min} = \operatorname{lcm}(\lambda_1, \lambda_2) = k(k-1)/c_1c_2 \gcd(k, v)$
  $c_1 = \gcd(k, v-1)$
  $c_2 = \gcd(k-1, v-1)$
  $\lambda_1 = (k-1)/\gcd(k-1, v-1)$
  $\lambda_2 = k(k-1)/\gcd(k(k-1), v(v-1))$

Necessary Conditions for Simple BIBDs

Necessary conditions for a simple (v, k, λ) BIBD:

(1) $\lambda(v-1) \equiv 0 \mod (k-1)$
(2) $\lambda v(v-1) \equiv 0 \mod k(k-1)$
(3) $\lambda_{min} \leq \lambda \leq \lambda_{max} = \binom{v-2}{k-2}$

(Dehon 1983) There exists a simple $(v, 3, \lambda)$ BIBD if and only if $\lambda(v-1) \equiv 0 \pmod 2$, $\lambda v(v-1) \equiv 0 \pmod 6$, and $\lambda \leq v-2$.

Question: *Fix the number of elements v and a block size k. Under what circumstances will simple (v, k, λ) BIBDs exist for all λ satisfying the conditions (1) through (3)?*

Simple $(7,3,1)$ BIBD

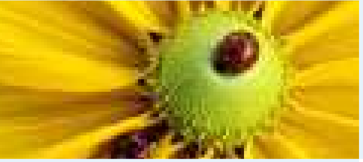
$$1,2,4$$
$$2,3,5$$
$$3,4,6$$
$$4,5,0$$
$$5,6,1$$
$$6,0,2$$
$$0,1,3$$

- from lines in a projective plane
- from a difference set $\{1,2,4\}$ in Z_7
- from partitioning a $(7,3,2)$ BIBD

Simple $(7, 3, 2)$ BIBD

$1, 2, 4$	$3, 5, 6$
$2, 3, 5$	$4, 6, 0$
$3, 4, 6$	$5, 0, 1$
$4, 5, 0$	$6, 1, 2$
$5, 6, 1$	$0, 2, 3$
$6, 0, 2$	$1, 3, 4$
$0, 1, 3$	$2, 4, 5$

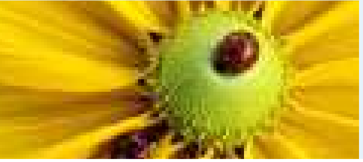
- from a difference family $\{1, 2, 4\}, \{3, 5, 6\}$ in Z_7
- the orbit of $\{1, 2, 4\}$ under the action of $Aff(Z_7)$



Simple $(7, 3, 3)$ BIBD

$0, 1, 4$	$0, 1, 2$	$0, 3, 5$
$1, 2, 5$	$1, 2, 3$	$1, 4, 6$
$2, 3, 6$	$2, 3, 4$	$2, 5, 0$
$3, 4, 0$	$3, 4, 5$	$3, 6, 1$
$4, 5, 1$	$4, 5, 6$	$4, 0, 2$
$5, 6, 2$	$5, 6, 0$	$5, 1, 3$
$6, 0, 3$	$6, 0, 1$	$6, 2, 4$

- from a difference family $\{0, 1, 4\}, \{0, 1, 2\}, \{0, 3, 5\}$ in Z_7
- the orbit of $\{0, 1, 4\}$ under the action of $Aff(Z_7)$



All Simple $(7, 3, \lambda)$ BIBDs Exist

- two simple $(7, 3, 1)$ BIBDs from one simple $(7, 3, 2)$ BIBD
- one simple $(7, 3, 3)$ BIBD
- they are disjoint

The list $\Gamma = (1, 1, 3)$ can represent numbers from 1 to 5.

Some Existence Theorems

Existence Theorem 1

(Theorem 2.6, Sun 2016)

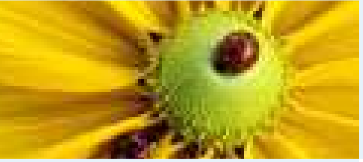
- q: a power p^α of an odd prime
- $3 \le k \le q-3$, $p \nmid k$
- $c_1 = \gcd(k, q-1)$, $c_2 = \gcd(k-1, q-1)$
- $\{c_1, c_2\} \cap \{1, 2\}$ is not empty
- There is a set D of some proper divisors of $c_1 c_2$ such that
  (1) $\sum_{d \in D} d \ge c_1 c_2 - 1$;
  (2) every number i with $1 \le i \le \sum_{d \in D} d$ can be expressed as a sum of distinct elements chosen from D.

Then the necessary conditions are also sufficient for the existence of a simple (q, k, λ) BIBD.

Existence Theorem 2

(Theorem 2.7, Sun 2016)

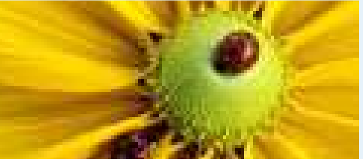
- q: a power p^α of an odd prime
- Let $\beta \geq 3$ be odd
- $\ell\beta^m \leq k \leq q - \ell\beta^m$, $p \nmid k$
- $c_1 = \gcd(k, q-1)$, $c_2 = \gcd(k-1, q-1)$, $m \geq 1$
- $\{c_1, c_2\} = \{1, \ell\beta^m\}$
- $\ell \geq 4$ is an even number with the following property:
  there is a set D of some proper divisors of ℓ such that
  (1) $\sum_{d \in D} d \geq \ell - 1$;
  (2) every number i with $1 \leq i \leq \sum_{d \in D} d$ can be expressed as a sum of distinct elements chosen from D.



Existence Theorem 2 conti.

Then, the necessary conditions are also sufficient for the existence of a simple (q, k, λ) BIBD if
$q > \beta^m(\sqrt{3(\beta - 1)/\delta + 1/4} + 3/2)$,
where $\delta = 1 - \sum_{\substack{h|\ell \\ h\,\mathrm{prime}}} (h^{k/\beta^m h})^{-1}$.

More specifically, this is the case when
$q > \beta^m(\sqrt{6\beta - 23/4} + 3/2)$.



Existence Theorem 3

(Theorem 2.8, Sun 2016)

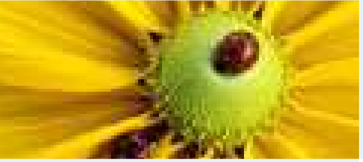
- q: a power p^α of an odd prime
- Let $\ell, \beta \geq 3$ be odd
- $\ell\beta^m \leq k \leq q - \ell\beta^m$, $p \nmid k$
- $c_1 = \gcd(k, q-1)$, $c_2 = \gcd(k-1, q-1)$, $m \geq 1$
- $\{c_1, c_2\} = \{2, \ell\beta^m\}$
- 2ℓ satisfies the following property:
  there is a set D of some proper divisors of 2ℓ such that
  (1) $\sum_{d \in D} d \geq 2\ell - 1$;
  (2) every number i with $1 \leq i \leq \sum_{d \in D} d$ can be expressed as a sum of distinct elements chosen from D.

Existence Theorem 3 conti.

Then, the necessary conditions are also sufficient for the existence of a simple (q, k, λ) BIBD if
$q > \beta^m(\sqrt{3(\beta - 1)/\delta + 1/4} + 3/2)$,
where $\delta = 1 - \sum_{\substack{h \mid \ell \\ h \text{ prime}}} (h^{k/\beta^m h})^{-1}$.

More specifically, this is the case when
$q > \beta^m(\sqrt{6\beta - 23/4} + 3/2)$.

Practical Numbers



Definition, Srinivasan 1948

A *practical number* (or *panarithmic number*) is a positive integer m such that every number less than m can be represented as a sum of distinct divisors of m.

$1, 2, 4, 6, 8, 12, 16, 18, 20, 24, 28, 30, 32, 36, 40, 42, 48, 54, 56, 60, 64, 66, 72, 78, 80, 84, 88, 90, 96, 100, 104, 108, 112, 120, 126, 128, 132, 140, 144, 150, 156, 160, 162, 168, 176, 180, 192, 196, 198, 200$, etc.

See: Melfi's tables

Theorem 4

(Melfi 1995, Sierpinski 1955, Stewart 1954)
Suppose $m = p_1^{e_1} p_2^{e_2} \cdots p_n^{e_n} \geq 2$ where $2 = p_1 < p_2 < \cdots < p_n$ and $e_i \geq 1$. The following conditions are equivalent.

(1) m is a practical number.

(2) Every number less than $\sigma(m)$ can be represented as a sum of distinct divisors of m, where $\sigma(x)$ denotes the sum of the divisors of x.

(3) $n = 1$ or $p_{i+1} \leq \sigma(p_1^{e_1} \cdots p_i^{e_i}) + 1$ for $1 \leq i \leq n - 1$.

Condition (3) brings a convenient numerical method for checking whether a number is practical or not, as long as we know its factorization.

Lemma 5, Margenstern 1991

Let m be a practical number. Then $\sigma(m) \geq 2m - 1$. Furthermore, $\sigma(m) \geq 2m$ if m is not a power of 2.

Lemma 6

Let $n \geq 2$ and let $L = (d_1 = 1, d_2, \ldots, d_n)$ be an increasing list of numbers. Then, every number i with $1 \leq i \leq \sum_{j=1}^{n} d_j$ can be expressed as a sum of elements chosen from L if and only if $(\sum_{j=1}^{h} d_j) + 1 \geq d_{h+1}$ for $h = 1, \ldots, n-1$.

New Results

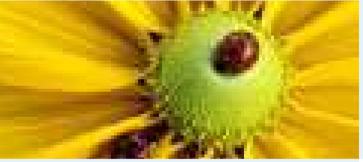
Theorem 7

Suppose $m \geq 2$. Then, m is a practical number if and only if there is a set D of some proper divisors of m such that (1) $\sum_{d \in D} d \geq m - 1$; (2) every number i with $1 \leq i \leq \sum_{d \in D} d$ can be expressed as a sum of distinct elements chosen from D.

Main Theorem

- q: a power p^α of an odd prime
- $3 \leq k \leq q-3$, $p \nmid k$
- $c_1 = \gcd(k, q-1)$, $c_2 = \gcd(k-1, q-1)$
- $\{c_1, c_2\} \cap \{1, 2\}$ is not empty

Then, the necessary conditions are also sufficient for the existence of a simple (q, k, λ) BIBD in any of the following situations.

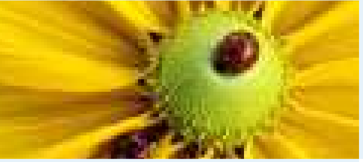


Main Theorem conti.

1. $c_1 c_2$ is a practical number.
2. $\{c_1, c_2\} = \{1, \ell\beta^m\}$, where
   (a) $\beta \geq 3$ is odd and $\ell \geq 4$ is a practical number;
   (b) $q > \beta^m(\sqrt{6\beta - 23/4} + 3/2)$ or
   $q > \beta^m(\sqrt{3(\beta - 1)/\delta + 1/4} + 3/2)$ with
   $\delta = 1 - \sum_{\substack{h|\ell \\ h \text{ prime}}} (h^{k/\beta^m h})^{-1}$.
3. $\{c_1, c_2\} = \{2, \ell\beta^m\}$, where
   (a) $\ell, \beta \geq 3$ are odd and 2ℓ is a practical number;
   (b) $q > \beta^m(\sqrt{6\beta - 23/4} + 3/2)$ or
   $q > \beta^m(\sqrt{3(\beta - 1)/\delta + 1/4} + 3/2)$ with
   $\delta = 1 - \sum_{\substack{h|\ell \\ h \text{ prime}}} (h^{k/\beta^m h})^{-1}$.

Example 2

1. A simple $(89, 44, 43i)$ BIBD exists for any i with $1 \leq i \leq \binom{87}{42}/43$. Note that $89 > \beta^m(\sqrt{6\beta - 23/4} + 3/2)$ is not valid when $\beta = 11$. However, the other inequality applies for this case.
2. A simple $(353, 45, 45i)$ BIBD exists for any i with $1 \leq i \leq \binom{351}{43}/45$.
3. A simple $(307, 51, 25i)$ BIBD exists for any i with $1 \leq i \leq \binom{305}{49}/25$.
4. A simple $(307, 52, 26i)$ BIBD exists for any i with $1 \leq i \leq \binom{305}{50}/26$.



Corollary 8

Let $\ell \geq 4$ be a practical number. Suppose $q = \ell h + 1$ is a power of an odd prime such that $\gcd(\ell - 1, h) = 1$. Then, a simple $(q, \ell, (\ell - 1)i)$ BIBD exists for any i with $1 \leq i \leq \binom{q-2}{\ell-2}/(\ell - 1)$.

Examples:
Let $q = 20h + 1$ be a power of an odd prime such that $19 \nmid h$. Then, a simple $(q, 20, 19i)$ BIBD exists for any i with $1 \leq i \leq \binom{q-2}{18}/19$. Some of the valid q are 41, 61, 81, 101, 121, 181, 241, 281, 361, 401, 421, 461, 521, 541, 601, 641, 661, 701, 821, 841, 881, 941, 961.

Corollary 9

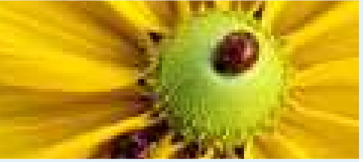
Let $\ell \geq 4$ be a practical number. Suppose $q = \ell h + 1 = p^\alpha$ is a power of an odd prime such that $\gcd(\ell + 1, ph) = 1$. Then, a simple $(q, (\ell + 1), (\ell + 1)i)$ BIBD exists for any i with $1 \leq i \leq \binom{q-2}{\ell-1}/(\ell + 1)$.

Examples:
Let $q = 40h + 1 = p^\alpha$ be a power of an odd prime such that $41 \nmid ph$. Then, a simple $(q, 41, 41i)$ BIBD exists for any i with $1 \leq i \leq \binom{q-2}{39}/41$. Some of the valid q are 81, 121, 241, 281, 361, 401, 521, 601, 641, 761, 841, 881, 961.

Corollary 10

Let 2ℓ be a practical number such that $\ell \geq 3$ is odd. Suppose $q = 2\ell h + 1$ is a power of an odd prime such that $\gcd(\ell - 1, h) = 1$. Then, a simple $(q, \ell, (\ell - 1)i/2)$ BIBD exists for any i with $1 \leq i \leq 2\binom{q-2}{\ell-2}/(\ell - 1)$.

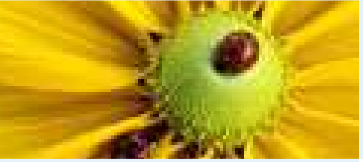
Examples:
Let $q = 18h + 1$ be a power of an odd prime such that $2 \nmid h$. Then, a simple $(q, 9, 4i)$ BIBD exists for any i with $1 \leq i \leq \binom{q-2}{7}/4$. Some of the valid q are 127, 163, 199, 271, 307, 343, 379, 487, 523, 631, 739, 811, 883, 919, 991.



Corollary 11

Let 2ℓ be a practical number such that $\ell \geq 3$ is odd. Suppose $q = 2\ell h + 1 = p^\alpha$ is a power of an odd prime such that $\gcd(\ell + 1, ph) = 1$. Then, a simple $(q, (\ell + 1), (\ell + 1)i/2)$ BIBD exists for any i with $1 \leq i \leq 2\binom{q-2}{\ell-1}/(\ell + 1)$.

Examples:
Let $q = 30h + 1$ be a power of an odd prime such that $2 \nmid h$. Then, a simple $(q, 16, 8i)$ BIBD exists for any i with $1 \leq i \leq \binom{q-2}{14}/8$. Some of the valid q are 151, 211, 271, 331, 571, 631, 691, 751, 811, 991.



References

References

- H.-M. Sun, From planar nearrings to generating blocks, Taiwanese J Math 14(5) (2010), 1713–1739.
- H.-M. Sun, On the existence of simple BIBDs with number of elements a prime power, J Combin Des 21(2) (2013), 47–59.
- H.-M. Sun, Correction to: "On the existence of simple BIBDs with number of elements a prime power", J Combin Des 21(10) (2013) 478–479.

References Conti.

- H.-M. Sun, More results on the existence of simple BIBDs with number of elements a prime power, Taiwanese J Math 20(3) (2016), 523–543.

- H.-M. Sun, Existence of simple BIBDs from the existence of a prime power difference family with minimum index, J Algebra Appl 18(9) (2019), Article 1950166.

The End.