

## SUM PACKING AND GRIGGS' THEOREM ON SUMS OF RESIDUES

MICHEL BOYER

**ABSTRACT.** This note first defines Sperner systems and presents a proof of Sperner's theorem based on symmetric chains using an approach similar to Griggs' in his article on the distributions of sums or residues modulo  $q$ . Then a detailed proof of Grigg's theorem is presented.

### 1. GENERALITIES

**1.1. Notations.** For an integer  $n$  we denote  $[n]$  the set  $[1..n]$  of integers from 1 to  $n$  and  $\mathbf{n}$  the set  $[0..n-1]$  of  $n$  elements;  $\mathbf{2} = \{0, 1\}$  and  $\mathbf{2}^n$  is the set of bitstrings of length  $n$ . We denote  $2^{[n]}$  the set of all subsets of  $[n]$ . There is a 1-1 correspondance between  $\mathbf{2}^n$  and  $2^{[n]}$ : which, to each bitstring  $x$ , associates the set of positions in the string where there is a 1: if  $n = 5$ , the bitstring 01101 corresponds to the set  $\{2, 3, 5\}$ . Subsets of  $[n]$  and bitstrings can thus be used interchangeably.

If  $X$  is a set  $|X|$  denotes the number of elements in  $X$ . For strings, it corresponds to the Hamming weight; for bitstring  $x$  it is  $|x| = \sum_i x_i$ .

**1.2. Sperner systems.** A subset  $\mathcal{A} \subseteq 2^{[n]}$  is called *Sperner system*<sup>1</sup> or *antichain* if all the elements of  $\mathcal{A}$  are non comparable i.e. for any distinct elements  $A$  and  $A'$  of  $\mathcal{A}$ ,  $A \not\subseteq A'$  and  $A' \not\subseteq A$ . Clearly if  $\emptyset \in \mathcal{A}$  then  $\mathcal{A} = \{\emptyset\}$  and, in the litterature, Sperner systems are often restricted to contain only non empty sets; we will not impose that restriction.

**1.3. Chains.** A chain  $\mathcal{C}$  is a subset of  $2^{[n]}$  whose elements are all comparable, i.e.  $\mathcal{C}$  is totally ordered by inclusion. Chains thus take the form

$$\mathcal{C} = \{C_0, \dots, C_r\}$$

where  $C_0 \subsetneq C_1 \dots \subsetneq C_r \subsetneq [n]$ . The integer  $r = |\mathcal{C}| - 1$  is called the *length* of the chain. We can of course replace subsets of  $[n]$  by bitstrings of length  $n$ . Then  $\mathcal{C}$  is a chain if  $C_{i+1}$  is obtained from  $C_i$  by replacing some zeros by ones. Here is a chain of length 2 in  $\mathbf{2}^5$ :

$$\mathcal{C} = \{10000, 10100, 11110\}$$

with strings of Hamming weight 1, 2 and 4 respectively.

**1.4. Symmetric chains.** A chain  $\mathcal{C} = \{C_0, \dots, C_r\} \subseteq \mathbf{2}^n$  is said to be *symmetric* if it contains sets of all sizes from  $|C_0|$  to  $|C_r|$  and  $|C_r| = n - |C_0|$ . In terms of bitstrings, a chain  $\mathcal{C} \subseteq \mathbf{2}^n$  is symmetric if the Hamming weight of its bitstrings go from  $u$  to  $n - u$  (without gap) for  $u = |C_0|$ . Here is a symmetric chain of  $\mathbf{2}^5$ :

$$\{00100, 10100, 10110, 10111\}$$

with strings whose set of Hamming weights is  $[1..4]$  (corresponding to the chain of sets  $\{\{3\}, \{1, 3\}, \{1, 3, 4\}, \{1, 3, 4, 5\}\}$ ). The set of weights of the strings in a symmetric chain  $\mathcal{C}$  being  $[u..n-u]$ , the number of strings in  $\mathcal{C}$  is thus  $l = n - 2u + 1$  and  $l$  is even if  $n$  is odd and odd if  $n$  is even. The interval of weigths is then  $\left[ \frac{n-l+1}{2} .. \frac{n+l-1}{2} \right]$  which can also be written

$$(1) \quad I_{n,l} = \left[ \lceil (n-l)/2 \rceil .. \lfloor (n+l)/2 \rfloor - 1 \right]$$

Notice that all  $k \in [0..n]$ ,  $I_{n,k}$  given by (1) contains  $k$  elements and  $k \mapsto I_{n,k}$  from  $[0..n]$  to  $2^{[n]}$  is strictly increasing.

**1.5. Partitions with symmetric chains.** A partition  $\mathcal{P}$  of a set  $X$  is a decomposition of  $X$  in non empty subsets that do not overlap. More precisely, it is a set of subsets of  $X$  such that  $X$  is the union of those subsets and no two of those subsets have an element in common (the subsets are pairwise disjoint). If  $X = \mathbf{2}^n$  and if we restrict the subsets to be symmetric chains, we speak of partitions with symmetric chains. With  $n = 4$  here is such a partition  $\mathcal{P}$  of  $\mathbf{2}^4$ :

$$\begin{aligned} & \{ \\ & \{0000, 1000, 1100, 1110, 1111\}, \\ & \{0001, 1001, 1101\}, \\ & \{0010, 1010, 1011\}, \\ & \{0100, 0110, 0111\}, \\ & \{0011\}, \\ & \{0101\} \\ & \} \end{aligned}$$

### 2. SPERNER'S THEOREM AND RELATED RESULTS

The partition of the previous section was obtained using the construction of the following proposition.

**Proposition 2.1.** *For all  $n \geq 1$  there is a partition of  $\mathbf{2}^n$  with symmetric chains.*

The following proposition is the key result that allows using symmetric chains to obtain Sperner's theorem and some of its generalisations.

**Proposition 2.2.** *Let  $w : \mathbf{2}^n \rightarrow \mathbf{N}$  be defined by  $w(x) = |x|$ . For any partition  $\mathcal{P}$  of  $\mathbf{2}^n$  such that for all  $\mathcal{S} \in \mathcal{P}$ ,  $w|_{\mathcal{S}}$  is 1-1 and  $w(\mathcal{S}) = I_{n,|\mathcal{S}|}$*

$$\sum_{\mathcal{S} \in \mathcal{P}} \min(k, |\mathcal{S}|) \leq \sum_{i \in I_{n,k}} \binom{n}{i}$$

Date: Oct 24, 2004.

<sup>1</sup>Sperner [1928]

*Proof.* Since  $k \mapsto I_{n,k}$  is increasing on  $[0..n]$ , the conditions of the proposition imply

$$\min(k, |\mathcal{S}|) = |w_{|\mathcal{S}|}^{-1}(I_{n,k})| = |\mathcal{S} \cap w^{-1}(I_{n,k})|$$

As a consequence, using the fact that  $\mathcal{P}$  is a partition,

$$\sum_{\mathcal{S} \in \mathcal{P}} \min(k, |\mathcal{S}|) = \sum_{\mathcal{S} \in \mathcal{P}} |\mathcal{S} \cap w^{-1}(I_{n,k})| = |w^{-1}(I_{n,k})| = \sum_{i \in I_{n,k}} |w^{-1}(\{i\})|$$

We end by saying that  $w^{-1}(\{i\})$  is exactly those strings in  $\mathbf{2}^n$  whose Hamming weight is  $i$  and their number is thus  $\binom{n}{i}$ .  $\square$

Notice that the  $\binom{n}{i}$  for  $i \in I_{n,k}$  are the  $k$  largest binomial coefficients. Notice also that a partition with symmetric chains satisfies the conditions of the proposition.

We can now deduce theorems that seem to be proven differently in the literature.

**Theorem 2.3** (Erdős). *If  $\mathcal{G} \subseteq \mathbf{2}^n$  contains no chain of length  $k$ , then  $|\mathcal{G}|$  is at most the sum of the  $k$  largest binomial coefficients  $\binom{n}{i}$ .*

*Proof.* Let  $\mathcal{P}$  be a partition of  $\mathbf{2}^n$  with symmetric chains. Since every subset of a chain is a chain, for all  $\mathcal{C} \in \mathcal{P}$ ,  $|\mathcal{G} \cap \mathcal{C}| \leq \min(k, |\mathcal{C}|)$  and

$$|\mathcal{G}| = \sum_{\mathcal{C} \in \mathcal{P}} |\mathcal{G} \cap \mathcal{C}| \leq \sum_{\mathcal{C} \in \mathcal{P}} \min(k, |\mathcal{C}|) \leq \sum_{i \in I_{n,k}} \binom{n}{i} \quad \square$$

**Theorem 2.4** (Sperner). *If  $\mathcal{A}$  is an antichain, then  $|\mathcal{A}| \leq \binom{n}{\lfloor n/2 \rfloor}$ .*

*Proof.* Just apply Theorem 2.3 with  $k = 1$ .  $\square$

**Theorem 2.5** (Erdős). *If  $\mathcal{G} \subseteq \mathbf{2}^n$  contains no two members  $A \supseteq B$  with  $|A - B| \geq k$ , then  $|\mathcal{G}|$  is at most the sum of the  $k$  largest binomial coefficients.*

*Proof.* The condition implies again that if  $\mathcal{P}$  is a partition of  $\mathbf{2}^n$  with symmetric chains, then  $\mathcal{G} \cap \mathcal{C}$  contains at most  $k$  elements for all  $\mathcal{C} \in \mathcal{P}$ .  $\square$

### 3. GRIGGS' THEOREM ON SUMS OF RESIDUES

We now follow Griggs [1993]. This will look like a repetition of the previous section except that Hamming weights are replaced by Hamming weights *modulo*  $q$ . Chains will be replaced by *structures*; notice that in Proposition 2.2, we needed only that  $w_{|\mathcal{S}|} : \mathcal{S} \rightarrow I_{n,|\mathcal{S}|}$  to be 1-1 and onto. This is the property that characterises structures.

**3.1. Structures.** Let  $\mathbf{Z}/q\mathbf{Z}$  be the ring of integers modulo  $q$  and for  $n \in \mathbf{Z}$ ,  $\pi_q(n) = \bar{n}$ , the class of  $n$  modulo  $q$ . Let also

$$\sigma : \{0, 1\}^n \rightarrow \mathbf{Z}/q\mathbf{Z}$$

be defined by  $\sigma = \pi_q \circ w$  i.e.  $\sigma(x) = \overline{|x|}$  is the class modulo  $q$  of the Hamming weight of the string  $x$ . A  $\sigma$ -structure is a subset  $\mathcal{S} \subseteq \mathbf{2}^n$  such that the restriction  $\sigma_{|\mathcal{S}}$  of  $\sigma$  to  $\mathcal{S}$  is injective; this means that if  $x, x' \in \mathcal{S}$  and  $|x| \equiv |x'| \pmod{q}$  then  $x = x'$  (no two strings in a structure have Hamming weights that are congruent modulo  $q$ ). A structure is  $\sigma$ -symmetric if

$$\sigma(\mathcal{S}) = \pi_q(I_{n,|\mathcal{S}|})$$

This is equivalent to saying that  $|\mathcal{S}| = q$  or there are  $u, v$  such that  $u + v = n$  and  $\sigma(\mathcal{S}) = \pi_q([u, v])$ .

**Proposition 3.1.** *If  $q > 1$  and  $n \geq 1$ , then there is a partition  $\mathcal{P}$  of  $\mathbf{2}^n$  by  $\sigma$ -symmetric structures.*

*Proof.* If  $n = 1$  the partition  $\{\{0, 1\}\}$  containing just one structure satisfies the condition. Let us assume by induction that there is a partition  $\mathcal{P}_{n-1}$  of  $\mathbf{2}^{n-1}$  by  $\sigma$ -symmetric structures. For each  $\mathcal{S}_i \in \mathcal{P}$  we construct two structures of  $\mathbf{2}^n$  as follows:  $\mathcal{S}'_i = \{x0 \mid x \in \mathcal{S}_i\}$  and  $\mathcal{S}''_i = \{x1 \mid x \in \mathcal{S}_i\}$ . If  $|\mathcal{S}_i| = q$  then  $|\mathcal{S}'_i| = |\mathcal{S}''_i| = q$ . Moreover  $\sigma$  is injective on both  $\mathcal{S}'_i$  and  $\mathcal{S}''_i$ . We thus keep both  $\mathcal{S}'_i$  and  $\mathcal{S}''_i$  as is. If  $|\mathcal{S}_i| < q$  then there are  $u, v$  such that  $u + v = n$  and  $\sigma(\mathcal{S}_i) = \pi_q([u..v])$  and then  $\sigma(\mathcal{S}'_i) = \pi_q([u..v])$  and  $\sigma(\mathcal{S}''_i) = \pi_q([u+1..v+1])$  and  $\sigma$  is injective on those two sets. We now need to rebalance. We take the element of  $\mathcal{S}''_i$  whose image is  $\pi_q(v+1)$  and move it to  $\mathcal{S}'_i$ . Now  $\mathcal{S}'_i$  is  $\sigma$ -symmetric, because  $\sigma(\mathcal{S}'_i) = \pi_q([u..v+1])$  with  $u+v+1 = n+1$ . It may happen that this empties  $\mathcal{S}''_i$  in which case we discard it. Else  $\mathcal{S}''_i$  is also  $\sigma$ -symmetric and we keep it. The  $\mathcal{S}'_i$  and  $\mathcal{S}''_i$  after discarding the empty  $\mathcal{S}''_i$  is a partition of  $\mathbf{2}^n$  by  $\sigma$ -symmetric structures.  $\square$

**Proposition 3.2.** *If  $\mathcal{P}$  is a partition of  $\mathbf{2}^n$  by  $\sigma$ -symmetric structures then*

$$\sum_{\mathcal{S} \in \mathcal{P}} \min(k, |\mathcal{S}|) \leq \sum_{i \in I_{n,k}} \binom{n}{i}_q$$

where  $\binom{n}{i}_q$  is the number of strings  $x \in \mathbf{2}^n$  such that  $|x| \equiv i \pmod{q}$ .

*Proof.* The map  $\sigma_{|\mathcal{S}} : \mathcal{S} \rightarrow \mathbf{Z}/q\mathbf{Z}$  is injective and its range is  $\pi_q(I_{n,|\mathcal{S}|})$ . For all  $k \geq 0$ ,  $\min(k, |\mathcal{S}|) = |\sigma_{|\mathcal{S}}^{-1}(I_{n,k})|$  and so

$$\sum_{\mathcal{S} \in \mathcal{P}} \min(k, |\mathcal{S}|) = \sum_{\mathcal{S} \in \mathcal{P}} |\sigma_{|\mathcal{S}}^{-1}(I_{n,k})| = |\sigma^{-1}(I_{n,k})|$$

and  $\sigma^{-1}(I_{n,k})$  is exactly those strings in  $x \in \mathbf{2}^n$  such that  $|x| \equiv i \pmod{q}$  for  $i \in I_{n,k}$ .  $\square$

**3.2. Griggs' theorem.** Let  $a_1, \dots, a_n$  be integers such that  $\gcd(a_i, q) = 1$  for  $i \in [1..n]$ . This is equivalent to saying that their classes  $\pi_q(a_i)$  are invertible in  $\mathbf{Z}/q\mathbf{Z}$  (and this is normally denoted  $\pi_q(a_i) \in (\mathbf{Z}/q\mathbf{Z})^*$ ). Griggs' theorem bounds the number of elements of the set

$$\left\{ x \in \mathbf{2}^n \mid \sum_{i=1}^n \pi_q(a_i)x_i \in E \right\}$$

for  $E \subseteq \mathbf{Z}/q\mathbf{Z}$ . If we let  $\sigma' : \mathbf{2}^n \rightarrow \mathbf{Z}/q\mathbf{Z}$  be defined by  $\sigma'(x) = \sum_{i=1}^n \pi_q(a_i)x_i$ , then this is equivalent to bounding  $|\sigma'^{-1}(E)|$ . Writing  $a'_i$  for  $\pi_q(a_i)$  we now state Griggs' theorem as follows:

**Theorem 3.3.** For  $a'_i \in (\mathbf{Z}/q\mathbf{Z})^*$  where  $i \in [1..n]$  let  $\sigma' : \mathbf{2}^n \rightarrow \mathbf{Z}/q\mathbf{Z}$  be defined by  $\sigma'(x) = \sum a'_i x_i$ . Then for any  $E \subseteq \mathbf{Z}/q\mathbf{Z}$

$$|\sigma'^{-1}(E)| \leq \sum_{i \in [1..n, |E|]} \binom{n}{i}_q$$

The proof will use a partition by sets on which  $\sigma'$  is injective and whose sizes are exactly those of the symmetric  $\sigma$ -structure we built inductively; the bound will follow by simple counting.

**Lemma 3.4.** Let  $S \subseteq \mathbf{Z}/q\mathbf{Z}$  with  $q > 1$  and  $S \neq \emptyset$ ; then for all  $a' \in (\mathbf{Z}/q\mathbf{Z})^*$ ,  $S + \{a'\} \subseteq S$  implies  $S = \mathbf{Z}/q\mathbf{Z}$ .

*Proof.* For any  $x \in S$ , the elements  $x + ka'$  must be in  $S$  for  $k \in [0..q-1]$ . Since  $a'$  is invertible, these elements are all distinct and fill  $\mathbf{Z}/q\mathbf{Z}$ .  $\square$

**Lemma 3.5.** Let  $\mathcal{P} = (\mathcal{S}_i)_{i \in [0..r]}$  be the partition of proposition 3.1. Let  $a'_i$  for  $i \in [1..n]$  be  $n$  invertible elements of  $\mathbf{Z}/q\mathbf{Z}$  and  $\sigma' : \mathbf{2}^n \rightarrow \mathbf{Z}/q\mathbf{Z}$  be defined by  $\sigma'(x) = \sum_{i=1}^n a'_i x_i$ . Then there is a partition  $\mathcal{P}' = (\mathcal{S}'_i)_{i \in [1..r]}$  such that  $|\mathcal{S}'_i| = |\mathcal{S}_i|$  for all  $i \in [1..r]$  and  $\sigma'$  is injective on every  $\mathcal{S}'_i$ .

*Proof.* We proceed by induction on  $n$ . For  $n = 1$ ,  $\mathcal{P}' = \mathcal{P}$ . Assume by induction that  $\mathcal{P}'_n$  is a partition of  $\mathbf{2}^n$  satisfying the conditions of the lemma for  $\{a'_1, \dots, a'_n\} \subseteq (\mathbf{Z}/q\mathbf{Z})^*$ . Let  $a'_{n+1} \in (\mathbf{Z}/q\mathbf{Z})^*$ . Given  $\mathcal{S}_i \in \mathcal{P}'_n$  we let  $\mathcal{S}'_i = \{x0 \mid x \in \mathcal{S}_i\}$  and  $\mathcal{S}''_i = \{x1 \mid x \in \mathcal{S}_i\}$ . Clearly  $\sigma'$  is injective on both  $\mathcal{S}'_i$  and  $\mathcal{S}''_i$  and the  $\mathcal{S}'_i$  and  $\mathcal{S}''_i$  form a partition of  $\mathbf{2}^{n+1}$ . If  $|\mathcal{S}_i| = q$  then  $\mathcal{S}'_i$  and  $\mathcal{S}''_i$  are left as is. Else, by the preceding lemma, there is a string  $x1 \in \mathcal{S}''_i$  such that  $\sigma'(x1)$  is different from all the  $\sigma'(x'0)$  with  $x' \in \mathcal{S}_i$ . We move that string from  $\mathcal{S}''_i$  to  $\mathcal{S}'_i$ ; if this empties  $\mathcal{S}''_i$  we just discard it. This is of course still a partition of  $\mathbf{2}^{n+1}$ ,  $\sigma'$  is injective on all its elements and we get inductively that the sizes of the elements of  $\mathcal{P}'$  are exactly those of  $\mathcal{P}$ .  $\square$

We now prove Griggs' theorem

*Proof.* Let  $\mathcal{P}'$  be a partition of  $\mathbf{2}^n$  satisfying the conditions of the preceding lemma. Then for any  $E \subseteq \mathbf{Z}/q\mathbf{Z}$

$$|\sigma'^{-1}(E)| = \sum_{i=1}^r |\sigma'_{|\mathcal{S}'_i}|^{-1}(E)| \leq \sum_{i=1}^r \min(|E|, |\mathcal{S}'_i|) = \sum_{i=1}^r \min(|E|, |\mathcal{S}_i|)$$

and the result now follows by Proposition 3.2.  $\square$

## REFERENCES

- Jerrold R. Griggs. On the distribution of sums of residues. *Bulletin of the American Mathematical Society*, 28(2):329–333, April 1993. math.NT/9304211.
- E. Sperner. Ein Satz über Untermenge einer endlichen Menge. *Math. Z.*, 27:544–548, 1928.