

## Hypercube problems

### Lecture 10

December 12, 2012

Lecturer: Petr Gregor

Scribe by: Václav Vlček

Updated: March 18, 2016

## 1 Gray codes

In a broader context, the term *Gray code* denotes enumerating all objects of some class into a sequence so that consecutive objects differ only by a “small amount”. For example, it is possible to generate all permutations in  $S_n$  so that consecutive permutations differ by a single transposition. We will focus to the case of enumerating all binary strings of a fixed length so that consecutive strings differ in a single coordinate.

**Definition 1 (Gray code)** *A (cyclic) binary Gray code of dimension  $n$  is a Hamiltonian path (cycle) in  $Q_n$ .*

Let us mention some references where Gray codes appeared, mainly from the history of communication:

1872 L. A. Gross described [6] the mathematical background of so called *Chinese ring puzzle* (also known as *Baguenaudier*) which anticipated Gray codes,

1878 E. Baudot<sup>1</sup> used Gray codes to design a telegraphic alphabet (he used a code of dimension 5 to design an alphabet of 31 symbols),

1943 The idea of Gray codes is inherently present in the patent of G. Stibitz,

1953 F. Gray from Bell Labs patented [5] the code (the patent application was for a pulse code modulation tube which was used for analog transmission of digital signals).

One of the constructions of a Gray code is contained in the following definition and depicted on the following figure.

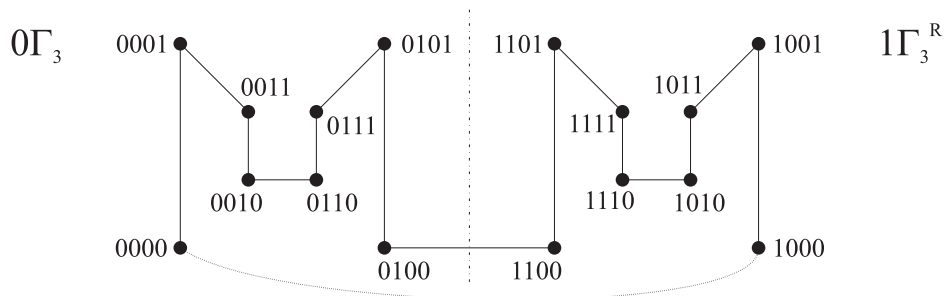
**Definition 2 (reflected Gray code)** *A reflected Gray code  $\Gamma_n$  is defined recursively:*

- $\Gamma_0 = \lambda$  (that is, an empty word),
- $\Gamma_{n+1} = (0\Gamma_n, 1\Gamma_n^R)$

where  $\Gamma_n^R$  denotes the reversed sequence  $\Gamma_n$ , and  $\alpha\Gamma$  denotes the sequence obtained from  $\Gamma$  by adding the symbol  $\alpha$  in front of each element of  $\Gamma$ .

---

<sup>1</sup>In his honor the unit for communication speed was named *baud*, denoted by Bd. (The number of bauds signifies the number of changes made to a transmission medium per second.)



We will use the following definitions. Let  $\Gamma_n = (v_0, \dots, v_{2^n-1})$  be the reflected Gray code of dimension  $n$ . For  $0 \leq i < 2^n$  let  $(i)_2$  denote the binary representation of  $i$  in  $n$  bits, and let  $\text{sh}_0(x) = 0x_1 \dots x_{n-1}$  for  $x \in \mathbb{Z}_2^n$  (that is, the right shift).

It is not hard to deduce formulae that tell how to compute the  $i$ -th element  $v_i$  of the reflected Gray code, and vice versa, how to compute the index  $i$  of a given element  $v_i$ . The proof is left as an exercise.

**Observation 3** For the reflected Gray code of dimension  $n$ ,

$$v_i = (i)_2 \oplus (\lfloor i/2 \rfloor)_2,$$

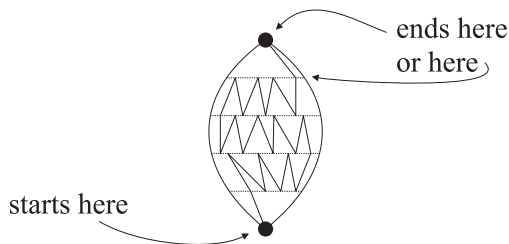
$$(i)_2 = v_i \oplus \text{sh}_0(v_i) \oplus \text{sh}_0^2(v_i) \oplus \dots \oplus \text{sh}_0^{n-1}(v_i).$$

## 2 Monotone Gray codes

In the following sections we study Gray codes that satisfy some additional requirements. We start with monotone Gray codes.

**Definition 4 (monotone Gray code)** A binary Gray code  $\Gamma = (v_1, \dots, v_{2^n})$  is monotone if  $|v_i| \leq |v_{i+2}|$  for every  $1 \leq i \leq 2^n - 2$ .

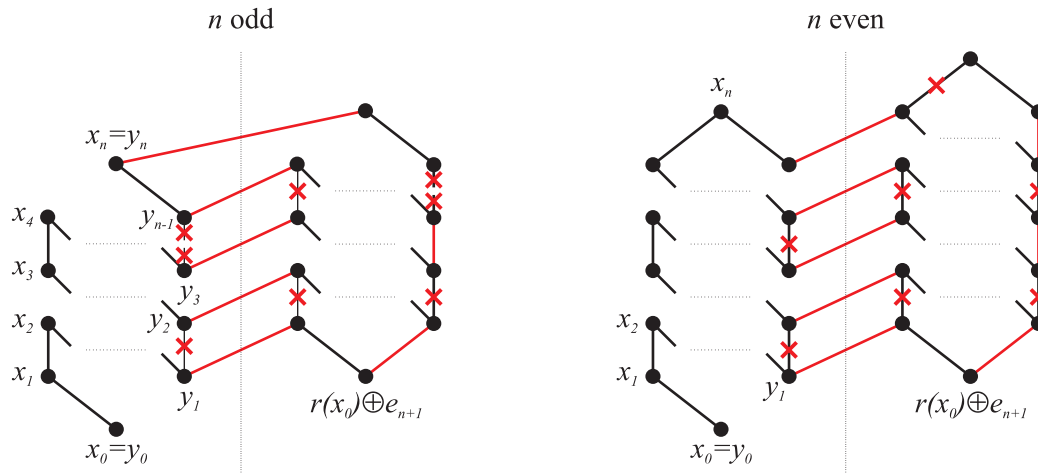
The idea of monotone Gray codes is illustrated on the figure below. The vertices of the hypercube are depicted in levels by their number of 1's. A monotone Gray starts in  $\mathbf{0}$  or in the first level (but in that case it goes to  $\mathbf{0}$  in the first step), afterwards it always has to oscillate between two consecutive levels until the lower one is entirely covered, and then it continues one level higher. Finally, it ends in  $\mathbf{1}$  or in the penultimate level.



**Theorem 5 (Savage, Winkler [15])**  $Q_n$  has a monotone Gray code for every  $n \geq 1$ .

**Proof** We construct recursively by  $n$  a monotone Gray code with chains  $X = (x_0 = \mathbf{0}, x_1, \dots, x_n = \mathbf{1})$ ,  $Y = (y_0 = \mathbf{0}, y_1, \dots, y_n = \mathbf{1})$  such that for every odd  $i$ , the edges  $x_i x_{i+1}$  and  $y_i y_{i+1}$  are the first and the last edge, respectively, of the code between levels  $i$  and  $i+1$ . For  $n = 1$  such code clearly exists.

For the induction step, let us assume that we have a such monotone Gray code of dimension  $n$  in  $Q_{n+1}^0$ . From the previous lectures we know that there is a rotation  $r \in R_n$  such that  $r(x_i) = y_i$ . In  $Q_{n+1}^1$  we take the same code rotated by  $r$ . The desired code will be created by joining this two codes together as depicted on the following figure.



■

**Remark** Monotone Gray codes have maximal number of peaks amongst all Gray codes. A *peak* of a path in  $Q_n$  is a subpath  $(x, y, z)$  with  $|x| = |z|$ .

The *middle level graph* in  $Q_{2k+1}$  is the subgraph induced by levels  $k$  and  $k+1$ .

**Corollary 6** ([15]) *The middle level graph in  $Q_{2k+1}$  has a path of length at least  $\binom{2k+1}{k}$ .*

The following well-known conjecture is known [16] to hold for every  $k \leq 17$ .

**Conjecture 7 (Havel [7])** *The middle level graph in  $Q_{2k+1}$  is Hamiltonian for all  $k \geq 1$ .*

Currently, the best known result shows that the conjecture holds “asymptotically”.

**Theorem 8 (Johnson [9])** *The middle level graph in  $Q_{2k+1}$  has a cycle of length at least  $(1 - \frac{c}{\sqrt{k}})2\binom{2k+1}{k}$  where  $c$  is some constant.*

We omit the proof, though we mention that it uses long cycles in hypercubes with small number of peaks, contrary to the monotone Gray codes. This also motivates the question of relation between Gray codes and (symmetric) chain decompositions.

**UPDATE:** The middle level conjecture has been proven by T. Mütze in 2014, see preprint [12].

### 3 Symmetric chain decomposition

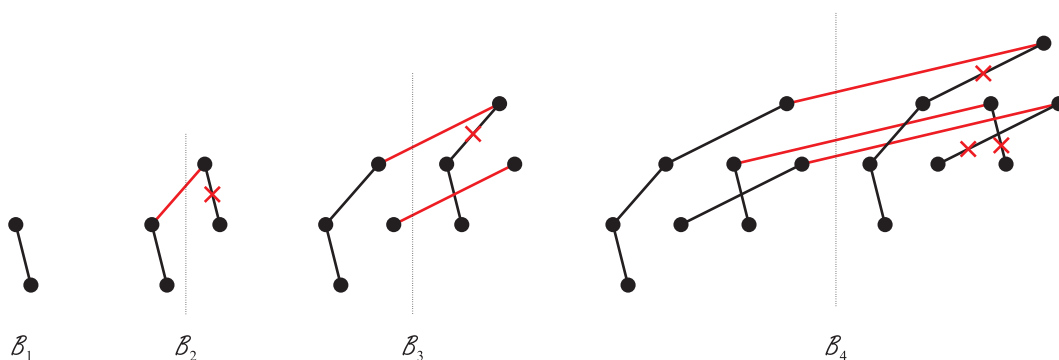
In this section we switch to the language of Boolean lattices  $\mathcal{B}_n = (\mathcal{P}([n]), \subseteq)$ .

**Definition 9** A symmetric chain in  $\mathcal{B}_n$  is a sequence of sets  $X_k \subset X_{k+1} \subset \dots \subset X_{n-k}$  with  $|X_i| = i$  for every  $k \leq i \leq n - k$ .

**Proposition 10**  $\mathcal{B}_n$  has a decomposition into symmetric chains for every  $n \geq 1$ .

**Proof** We proceed by induction on  $n$ . For  $n = 1$  the statement clearly holds since  $\mathcal{B}_1$  consists of a single symmetric chain  $(\emptyset, \{1\})$ .

For a symmetric chain  $C = (X_k, \dots, X_{n-k})$  in  $\mathcal{B}_n$  let  $C' = (X_k, \dots, X_{n-k}, X_{n-k} \cup \{n+1\})$  and if  $k < n/2$ , let  $C'' = (X_k \cup \{n+1\}, \dots, X_{n-k-1} \cup \{n+1\})$ . If  $k = n/2$  then  $C''$  is undefined. Note that  $C'$  and  $C''$  are symmetric chains in  $\mathcal{B}_{n+1}$ , see the figure below. Observe that if  $\mathcal{C}$  is a symmetric chain decomposition of  $\mathcal{B}_n$ , then  $\{C', C'' \mid C \in \mathcal{C}\}$  is a symmetric chain decomposition of  $\mathcal{B}_{n+1}$ .



■

By the definition, every symmetric chain intersects the middle level (both middle levels if  $n$  is odd). Thus, there is exactly  $\binom{n}{\lfloor n/2 \rfloor}$  chains in a symmetric chain decomposition. On the other hand, every pair of sets from the same level is incomparable (by inclusion); that is, a level forms an antichain. Since every antichain contains at most one set from each chain of the decomposition, we obtain the classical Sperner theorem.

**Corollary 11 (Sperner [19])** The maximal size of an antichain in  $\mathcal{B}_n$  is  $\binom{n}{\lfloor n/2 \rfloor}$ .

**Problem 12** Is it true that for every  $n$  some symmetric chain decomposition (the one above) can be extended to a (cyclic) Gray code?

**UPDATE:** This has been recently answered positively by Streib and Trotter, see [18].

**Problem 13 (Felsner, Trotter; see [8])** Is there a Gray code for every  $n$  satisfying the condition that if  $X \subseteq Y$  then  $X$  precedes  $Y$  or  $X$  follows immediately after  $Y$ ?

It is clear that a such Gray code has to be monotone. It is only known [2] that for every  $n \geq 1$  all subsets of  $[n]$  of size at most 3 can be ordered so that the condition holds.

## 4 Other special Gray codes

In this section we survey several special Gray codes with interesting properties, but we omit all proofs.

**Definition 14 (transitional sequence)** A transitional sequence of a cyclic Gray code  $\Gamma = (v_1, \dots, v_{2^n})$  is a sequence  $t(\Gamma) = (t_1, \dots, t_{2^n})$  over  $[n]$  such that  $v_i \oplus v_{i+1} = e_{t_i}$  for every  $1 \leq i \leq 2^n$  (we consider  $v_{2^n+1} = v_1$ ).

**Definition 15 (balanced Gray code)** A Gray code  $\Gamma$  is called (almost) balanced if every  $i \in [n]$  has the same number of occurrences in  $t(\Gamma)$  (respectively, they differ at most by 2).

**Theorem 16 ([1, 13, 20])** For every  $n \geq 1$  there is an almost balanced Gray code. In particular, for  $n = 2^k$  there is a balanced Gray code.

**Definition 17 (antipodal Gray code)** A Gray code  $\Gamma$  in  $Q_n$  is antipodal if every pair of antipodal vertices in  $Q_n$  is at distance exactly  $n$  in  $\Gamma$ .

**Theorem 18 (Kilian, Savage [10])** An antipodal Gray code in  $Q_n$  exists if  $n = 2^k$  and only if  $n$  is even.

Let us note that for  $n = 2^k$  the proof is constructive. On the other hand, it is known [10] that there is no antipodal Gray code for  $n = 6$ . Hence, it would be interesting to know whether  $n = 2^k$  is also a necessary condition.

**Problem 19 ([10])** Does an antipodal code in  $Q_n$  exist only if  $n = 2^k$ ?

**Definition 20** The graph  $G(\Gamma) = (V, E)$  induced by a Gray code  $\Gamma$  has the vertex set  $V = [n]$  and  $ij \in E$  if  $i$  and  $j$  are consecutive in the transitional sequence  $t(\Gamma)$ .

For example, the graph induced by the reflected Gray code in  $Q_n$  is a star  $K_{1, n-1}$ , with the central vertex  $n$ , since every second edge of the code has the direction  $n$ .

It is known [4] that for every  $n \leq 6$  there is a Gray code inducing the path  $P_n$  but there is no Gray code inducing  $P_7$ . Despite considerable effort, no Gray codes inducing longer paths have been found. That leads to the following conjecture.

**Conjecture 21 (Bultena, Ruskey [4], Slater [17])** For every  $n \geq 7$ , the path  $P_n$  is not inducible by a Gray code in  $Q_n$ .

Another interesting question [4] is whether there is a Gray code that induces a cycle  $C_n$  for every (large enough)  $n$ .

**Definition 22** For a Gray code  $\Gamma$ , the run length  $r(\Gamma)$  is the minimal number of steps in which some direction repeats in  $t(\Gamma)$ . Furthermore, a maximal run length in  $Q_n$  is

$$r(n) = \max\{r(\Gamma) \mid \Gamma \text{ is a Gray code in } Q_n\}.$$

**Problem 23 ([11])** Determine  $r(n)$  for every  $n$ .

The values of  $r(n)$  are known for  $n \leq 7$ , for example  $r(5) = 4$ . Furthermore, asymptotically it holds  $r(n) = n - O(\log n)$ .

## Notes

For Gray codes in a broader context, we refer to the survey of Savage [14]. A part of Knuth's famous monograph [11] is devoted to Gray codes which is recommended for further study. For example details of the proof of Observation 3 can be found there. Proposition 10 is involved in Kleitman's solution of the Littlewood-Offord problem, for details see e.g. [3].

## References

- [1] G. S. BHAT, C. D. SAVAGE, *Balanced Gray Codes*, Electron. J. Combin. 3 (1996), #R25.
- [2] C. BIRO, D. HOWARD, *The first three levels of an order-preserving Hamiltonian path in the subset lattice*, Order 26 (2009), 101–107.
- [3] B. BOLLOBÁS, *Combinatorics: set systems, hypergraphs, families of vectors, and combinatorial probability*, Cambridge University Press, Cambridge, 1986.
- [4] B. BULTENA, F. RUSKEY, *Transition restricted Gray codes*, Electron. J. Combin. 3 (1996), #R11.
- [5] F. GRAY, *Pulse Code Communication*, U.S. Patent 2,632,058, filed 13 November 1947, issued 17 March 1953.
- [6] L. A. GROSS, *Thorie du Baguenodier*, Aim Vingtrinier, Lyon, 1872.
- [7] I. HAVEL, *Semipaths in directed cubes*, in M. Fiedler (ed.), *Graphs and Other Combinatorial Topics*, Teubner, Leipzig, 1983, 101–108.
- [8] B. JACKSON, B. STEVENS, G. HURLBERT, *Research problems on Gray codes and universal cycles*, Discrete Math. 309 (2009), 5341–5348, Problem 483.
- [9] J. R. JOHNSON, *Long cycles in the middle two layers of the discrete cube*, J. Combin. Theory Ser. A 105 (2) (2004), 255–271.
- [10] C. E. KILLIAN, C. D. SAVAGE, *Antipodal Gray Codes*, Discrete Math. 281 (2002), 221–236.
- [11] D. E. KNUTH, *The Art of Computer Programming, Volume 4, Fascicle 2: Generating All Tuples and Permutations*, Addison-Wesley Professional, 2005.
- [12] T. MÜTZE, *Proof of the middle levels conjecture*, arXiv 1404.4442 (2014), preprint.
- [13] J. ROBINSON, M. COHN, *Counting Sequences*, IEEE Trans. Comput. C-30 (1981), 17–23.
- [14] C. D. SAVAGE, *A survey of combinatorial Gray codes*, SIAM Rev. 39 (1997), 605–629.
- [15] C. D. SAVAGE, P. WINKLER, *Monotone Gray code and the middle levels problem*, J. Combin. Theory Ser. A 70 (2) (1995), 230–248.

- [16] I. SHIELDS, B. J. SHIELDS, AND C. D. SAVAGE, *An update on the middle levels problem*, Discrete Math. 309 (2009), 5271–5277.
- [17] P. J. SLATER, *Research Problems 109 and 110*, Discrete Math. 76 (1989), 293–294.
- [18] N. STREIB, W. T. TROTTER, *Hamiltonian Cycles and Symmetric Chains in Boolean Lattices*, Graphs Combinator. 30 (2014), 1565–1586.
- [19] E. SPERNER, *Ein Satz über Untermengen einer endlichen Menge*, Math. Z. 27 (1928), 544–548.
- [20] D. G. WAGNER, J. WEST, *Construction of Uniform Gray Codes*, Congres. Numer. 80 (1991), 217–223.