Linear Programming for Binary Codes with Kravchuk Polynomial

Cheng-Han Huang (黃承瀚), *Dept. of Math., National Central University, Taiwan* (108201014@cc.ncu.edu.tw),
Yun-Hao Lee (李昀浩), *Dept. of Math., National Central University, Taiwan* (108201016@cc.ncu.edu.tw)

Advisor: Prof. Wei-Hsuan Yu (俞韋亘)

Abstract

An **[n,d] code** is a code of length n in which any two words have Hamming distance at least d. The **maximum** number of an [n,d] code is denoted by **A[n,d]**. We approach the upper bound of an A[n,d] problem by **using linear programming method**. Moreover, if some specific weight distribution W_i is known, then the upper bound can be smaller. In particular, we can prove A[10,4]=40 by the method.

Problem description

Consider the n-dimensional vector space over the field of two elements, $\{0,1\}^n$. The vectors in this space are called **words**. The **Hamming distance $d_H(x,y)$** between two words x and y is defined to be the number of coordinate places in which they differ. The **Hamming weight |x|** of a word x equals its distance to the origin. A subset $\{0,1\}^n$ is called a binary code of length n. An **[n,d,w] code** is an [n,d] code in which all words have weight w. For each $k,n \in \mathbb{N}$, the binary **Kravchuk polynomial** K_k of degree k is defined by $K_k(x) = \sum_j (-1)^j \binom{x}{j}\binom{n-x}{k-j}$, $\forall x \in \mathbb{R}$.

Given the length and minimum distance of a [n,d] code, we maximize the upper bound of A[n,d] by **linear programming method**. Consider constraints based on **Kravchuk polynomial**, we give an upper bound for all positive integers n and even positive integer d, where $n \geq d$, and by the theorem that $A(n-1,d-1) = A(n,d)$, we give an upper bound for all $n, d \in \mathbb{N}$.

Results and discussion

Case1: Optimize using Kravchuk Polynomial

The **distance distribution** is the sequence $(A_i)_{i=0}^n$ where A_i equals the average number of codewords at distance i from a fixed codeword, in other words,

$$A_i = \frac{1}{|C|}\sum_{x\in C}\left|\{y \mid y \in C \cap d_H(x,y) = i\}\right|.$$

From P. Delsarte [1], $\sum_{i=0}^{n} \mathbf{A_i K_k}(\mathbf{i}) \geq \mathbf{0}$ for all $k \in \{0,1,\dots,n\}$ holds for binary codes of length n and distance distribution $(A_i)_{i=0}^n$. Combining the important inequality with some other inequalities : $\mathbf{A_i \geq 0}$ for all $i \in \{1,2,\dots,n\}$, $\mathbf{A_0 = 1}$,and $\mathbf{A_i = 0}$ for all $i \in \{1,2,\dots,d-1\}$, for [n,d] codes, we have the **constraints** of $\mathbf{M=\sum_{i=0}^{n} A_i}$.By **convex optimization CVX** , we show that **A[10,4]=42.**

Now, the **weight distribution** is introduced and we can develop some constraints to improve the upper bound constrained by **Kravchuk polynomials**, where the new constraints give credit to M. R. Best [2].

Case 2: Adding extra constraints

The **weight distribution** of a code is the sequence $(W_i)_{i=0}^n$ where W_i equals the number of codewords of weight i. Considering the following lemma:
1.Let C be an [n,d] code with d even and with weight distribution $(W_i)_{i=0}^n$.
Furthermore, let P, Q, and R be upper bounds for $A[n-1,d,\frac{1}{2}d+1]$,$A[n-\frac{1}{2}d,d,\frac{1}{2}d+1]$, and $A[n-\frac{1}{2}d+2,d,\frac{1}{2}d+2]$, respective. Then

$$\mathbf{(\tfrac{1}{2}d+2)W_{n-(\frac{1}{2})d-2} + \tfrac{1}{2}d(P-Q)W_{n-(\frac{1}{2})d} + (nP-(\tfrac{1}{2}d+2)R)W_{n-(\frac{1}{2})d+2} + nP\sum_{i=n-(\frac{1}{2})d+3}^{n} W_i \leq nP.}$$

For n=10 and d=4, we have $\mathbf{4x_6 + 8x_8 \leq 120}$.
2. Let C be an [n,d] code with weight distribution $(W_i)_{i=0}^n$ .Then $\mathbf{\sum_{i=0}^{n} W_i \leq nA[n-1,d]}$.
For n=10 and d=4, we have $\mathbf{5 + 3x_4 + 2x_6 + x_8 \leq 100}$.

By adding the above inequalities, we show that **A[10,4]=40**.

Case 1

```
number of iterations   = 15
primal objective value =  4.26666667e+01
dual   objective value =  4.26666667e+01
gap := trace(XZ)       = 4.29e-09
relative gap           = 4.97e-11
actual relative gap    = 1.05e-11
rel. primal infeas (scaled problem)   = 3.04e-14
rel. dual     "        "       "      = 1.42e-09
rel. primal infeas (unscaled problem) = 0.00e+00
rel. dual     "        "       "      = 0.00e+00
norm(X), norm(y), norm(Z) = 4.4e+01, 2.7e+01, 5.6e+02
norm(A), norm(b), norm(C) = 5.0e+02, 3.2e+00, 2.4e+00
Total CPU time (secs)  = 0.07
CPU time per iteration = 0.00
termination code       =  0
DIMACS: 4.9e-14  0.0e+00  1.7e-09  0.0e+00  1.0e-11  5.0e-11
------------------------------------------------------------

------------------------------------------------------------
Status: Solved
Optimal value (cvx_optval): +42.6667
```

Case 2

```
number of iterations   = 15
primal objective value =  4.00000001e+01
dual   objective value =  4.00000000e+01
gap := trace(XZ)       = 6.22e-07
relative gap           = 7.68e-09
actual relative gap    = 1.96e-09
rel. primal infeas (scaled problem)   = 6.18e-10
rel. dual     "        "       "      = 3.33e-09
rel. primal infeas (unscaled problem) = 0.00e+00
rel. dual     "        "       "      = 0.00e+00
norm(X), norm(y), norm(Z) = 2.0e+00, 2.6e+01, 5.2e+02
norm(A), norm(b), norm(C) = 5.0e+02, 3.2e+00, 1.5e+02
Total CPU time (secs)  = 0.06
CPU time per iteration = 0.00
termination code       =  0
DIMACS: 1.0e-09  0.0e+00  4.2e-09  0.0e+00  2.0e-09  7.7e-09
------------------------------------------------------------

------------------------------------------------------------
Status: Solved
Optimal value (cvx_optval): +40
```

Conclusions

We give an upper bound for any [n,d] codes, independently not need to know any other information. By adding extra constraints, we can improve the bound and is possible to achieve some known actual value. However, the extra constraints do depend on the [n,d,w] cases, which is not trivial and has no general theorem to obtain the values.

References

[1]P. Delsarte, “Bounds for unrestricted codes, by linear programing,” Philips Res. Reports, vol 27, pp. 272-289, 1972.
[2]M. R. Best, “Binary codes with a minimum distance of four,”, IEEE Trans. Inform. Theory, vol. IT-26, pp. 738-742, 1980.