

Perfect single error-correcting codes in the Johnson scheme

Dan Gordon

IDA/CCR-La Jolla

January 30, 2007



- Codes in the Johnson Scheme
- Necessary conditions for perfect Johnson codes
- Powers in short intervals
- New bounds



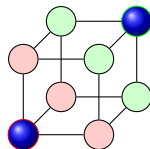
Codes in Graphs

Let $G = (V, E)$ be a graph.

Definition

A *code* is a subset of the vertices of G .

The standard example is G an n -cube.



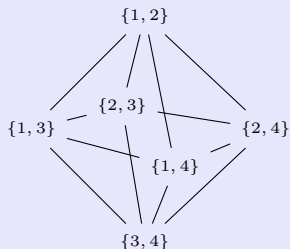
The Johnson Scheme

Definition

The Johnson graph $J(n, w)$:

- Vertices: w -subsets of $\mathcal{N} = \{1, 2, \dots, n\}$.
- Edges between sets with $w - 1$ common elements.
- distance
 $d(u, v) = w - |u \cap v|$.

Example: $J(4, 2)$



Definition

A code C is *perfect* if every vertex is distance $\leq e$ from *exactly* one codeword of C .

For the n -cube \mathbb{Z}_2^n , some perfect codes are

- repetition codes
- $[2^m - 1, 2^m - m - 1, 3]$ Hamming codes,
- The $[23, 12, 7]$ binary Golay code.
- The $[11, 6, 5]$ ternary Golay code.



Conjecture (Delsarte, 1973)

No nontrivial perfect codes exist in the Johnson scheme.



Perfect Johnson Scheme Codes

Conjecture (Delsarte, 1973)

No nontrivial perfect codes exist in the Johnson scheme.

Partial Results

- None for $e = 3, 7, 8$. (Etzion and Schwartz)
- None for $e = 1, n \leq 50000$.



Perfect Johnson Scheme Codes

Conjecture (Delsarte, 1973)

No nontrivial perfect codes exist in the Johnson scheme.

Partial Results

- None for $e = 3, 7, 8$. (Etzion and Schwartz)
- None for $e = 1, n \leq 50000$.

In this talk I will look at $e = 1$.



Sphere-packing Condition

Let $n = 2w + a$

Sphere Packing Condition

For a perfect 1-code,

$$\Phi_1(n, w) = 1 + w(w + a) \binom{n}{w}.$$



Definition

A code is *t-regular* if its blocks form a t -design $S_\lambda(t, w, n)$.



Strengthening the SPC

Definition

A code is *t-regular* if its blocks form a *t*-design $S_\lambda(t, w, n)$.

Theorem (Etzion and Schwarz)

A 1-perfect code is $L(w, a)$ -regular, where

$$L(w, a) = \frac{2w + a + 1 - \sqrt{(a + 1)^2 + 4(w - 1)}}{2}.$$



Strengthening the SPC (cont'd)

Corollary

If C is a perfect 1-code,

$$\Phi_1(w, a) = 1 + w(w + a) \mid \binom{2w + a - i}{w + a}$$

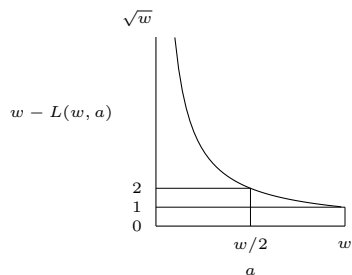
for $i = 0, 1, \dots, L(w, a)$.

So any prime dividing $\Phi_1(w, a)$ must divide **many** consecutive binomial coefficients.



$L(w, a)$

$$L(w, a) = \frac{2w + a + 1 - \sqrt{(a + 1)^2 + 4(w - 1)}}{2}.$$



Useful facts:

- $w \geq L(w, a) \geq w - \lceil \sqrt{w} \rceil$.
- $L(w, w/2) > w - 2$.



Divisors of $\Phi_1(w, a)$

Lemma (Kummer)

If $p^k \parallel \binom{a}{b}$, then adding b to $a - b$ in base p has k carries.

So if $p^k \parallel \Phi_1(w, a)$, then there are at least k carries when adding $w + a$ to $j = w - i$ for $j = \lceil \sqrt{w} \rceil, \lceil \sqrt{w} \rceil + 1, \dots, w$.



Divisors of $\Phi_1(w, a)$ (cont'd)

Denote the base p representation of $w + a$ by

$$w + a = (r_m, r_{m-1}, \dots, r_1, r_0)_p$$

Let $l = \lfloor m/2 \rfloor$.

Lemma

$r_i = p - 1$ for $i = l + 1, l + 2, \dots, m$.

Proof

Otherwise, adding p^i to $w + a$ has no carries.



Divisors of $\Phi_1(w, a)$ (cont'd)

Theorem

For any $p \mid \Phi_1(w, a)$, let $\alpha = m + 1 = \lfloor \log_p(w + a) \rfloor + 1$. Then

$$p^\alpha - \lceil \sqrt{w} \rceil - 1 \leq w + a < p^\alpha.$$



Divisors of $\Phi_1(w, a)$ (cont'd)

Theorem

For any $p \mid \Phi_1(w, a)$, let $\alpha = m + 1 = \lfloor \log_p(w + a) \rfloor + 1$. Then

$$p^\alpha - \lceil \sqrt{w} \rceil - 1 \leq w + a < p^\alpha.$$

Corollary

$$0 < \log_{w+a} p - \frac{1}{\alpha} < \frac{1}{\alpha} \left(\frac{1}{\sqrt{w+a}} + \frac{4}{(w+a)} \right).$$



Divisors of $\Phi_1(w, a)$ (cont'd)

Let

$$p_1 p_2 \dots p_r = \Phi_1(w, a) = 1 + w(w + a).$$

Theorem

$$\left| \sum_{i=1}^r \frac{1}{\alpha_i} - (1 + \log_{w+a} w) \right| < \frac{4}{\sqrt{w+a}}.$$



Divisors of $\Phi_1(w, a)$ (cont'd)

Let

$$p_1 p_2 \dots p_r = \Phi_1(w, a) = 1 + w(w + a).$$

Theorem

$$\left| \sum_{i=1}^r \frac{1}{\alpha_i} - (1 + \log_{w+a} w) \right| < \frac{4}{\sqrt{w+a}}.$$

For $0 < a < w/2$, we have $w + a < 3w/2$, so

$$1 - \log_{w+a} 3/2 < \log_{w+a} w < 1$$



Divisors of $\Phi_1(w, a)$ (cont'd)

Let

$$p_1 p_2 \dots p_r = \Phi_1(w, a) = 1 + w(w + a).$$

Theorem

$$\left| \sum_{i=1}^r \frac{1}{\alpha_i} - (1 + \log_{w+a} w) \right| < \frac{4}{\sqrt{w+a}}.$$

For $0 < a < w/2$, we have $w + a < 3w/2$, so

$$1 - \log_{w+a} 3/2 < \log_{w+a} w < 1$$

There are no 1-perfect codes with $n \leq 50000$, and so

$$\frac{1}{\alpha_1} + \frac{1}{\alpha_2} + \dots + \frac{1}{\alpha_r} \in [1.934, 2.026].$$



Divisors of $\Phi_1(w, a)$ (cont'd)

The smallest set of α 's is $\{1, 2, 3, 7\}$.

For such a perfect code to exist, we need p_1, p_2^2, p_3^3, p_4^7 all $\approx w + a$.

Conjecture (Loxton)

The number of perfect powers in $[x, x + \sqrt{x}]$ is bounded by a constant.

Best Bound (Loxton, Bernstein)

$$\exp\left(40\sqrt{\log \log x \log \log \log x}\right)$$



abc Conjecture

Let $\gamma(n)$ denote the largest squarefree divisor of n .

abc Conjecture

For any $\epsilon > 0$ there are only finitely many integers a , b and c such that $a + b = c$ and

$$\max\{a, b, c\} \geq C_\epsilon \gamma(abc)^{1+\epsilon}.$$

Theorem

The *abc* Conjecture implies there are only finitely many codes for a given $\alpha_1, \alpha_2, \dots, \alpha_r$.



A Computer Search

Since proving there are none seems hopeless, let's do a computer search.

Goal

Find all

$$p^a - q^b < \sqrt{p^a}$$

up to 2^L

We need only consider prime powers, since, for example, a 10th power is also a 5th.

This may be efficiently implemented with a priority queue.



Search Results

$p_1^{\alpha_1}$	$p_2^{\alpha_2}$	difference
2^7	5^3	3
13^3	3^7	10
3251^3	32^7	83883
33^7	3493^3	178820
1965781^3	498^7	1539250669

Pairs of Higher Powers in Short Intervals up to 2^{109}



Search Results

$p_1^{\alpha_1}$	$p_2^{\alpha_2}$	difference
2^7	5^3	3
13^3	3^7	10
3251^3	32^7	83883
33^7	3493^3	178820
1965781^3	498^7	1539250669

Pairs of Higher Powers in Short Intervals up to 2^{109}

Theorem

No perfect codes with $n < 2^{109}$.



Search Results (con'td)

This implies

$$\frac{1}{\alpha_1} + \frac{1}{\alpha_2} + \dots + \frac{1}{\alpha_r} \in [1.99, 2.001].$$

Corollary

At least two α_i 's have smallest prime factors ≥ 7 .



Search Results (con'td)

This implies

$$\frac{1}{\alpha_1} + \frac{1}{\alpha_2} + \dots + \frac{1}{\alpha_r} \in [1.99, 2.001].$$

Corollary

At least two α_i 's have smallest prime factors ≥ 7 .

Searching again with $p_1 = 7$ eliminated codes with $n < 2^{250}$.

