Aalto University
School of Science

More Differentially 6-uniform Power Functions

The differential spectrum of $x \mapsto x^{2^t-1}$ for some t.

Céline Blondeau and Léo Perrin

Tuesday, April 16

WCC 2013, *Bergen*

Outline

Differential Uniformity and Differential Spectrum

Previous work on the function $G_t(x) = x^{2^t-1}$

Spectrum of $G_t(x) = x^{2^t-1}$ when $t = \dfrac{n-1}{2}$ and $t = \dfrac{kn+1}{3}$

Conclusion

Outline

Differential Uniformity and Differential Spectrum

Previous work on the function $G_t(x) = x^{2^t-1}$

Spectrum of $G_t(x) = x^{2^t-1}$ when $t = \dfrac{n-1}{2}$ and $t = \dfrac{kn+1}{3}$

Conclusion

Differential uniformity [Nyberg 1993]

Let $F : \mathbb{F}_{2^n} \mapsto \mathbb{F}_{2^m}$. Then:

$$\delta(a, b) = \#\{x \in \mathbb{F}_{2^n},\ F(x + a) + F(x) = b\}$$

Differential uniformity of F :

$$\delta(F) = \max_{a \neq 0,\ b \in \mathbb{F}_{2^n}} \delta(a, b)$$

Almost-Perfect Non-linear (APN) function : $\delta(F) = 2$

Monomials

$$\begin{aligned} F_d : \quad \mathbb{F}_{2^n} &\to \mathbb{F}_{2^n} \\ x &\mapsto x^d \end{aligned}$$

Monomials

$$\begin{array}{rccc} F_d: & \mathbb{F}_{2^n} & \to & \mathbb{F}_{2^n} \\ & x & \mapsto & x^d \end{array}$$

- $\delta(a, b)$: number of roots of $x^d + (x + a)^d = b$
- For $a \neq 0$, $\delta(a, b) = \delta(1, b/a^d)$
  $\Rightarrow \delta(b) = \delta(1, b)$

Monomials

$$\begin{array}{rccc} F_d: & \mathbb{F}_{2^n} & \to & \mathbb{F}_{2^n} \\ & x & \mapsto & x^d \end{array}$$

- $\delta(a, b)$: number of roots of $x^d + (x + a)^d = b$
- For $a \neq 0$, $\delta(a, b) = \delta(1, b/a^d)$
  $$\Rightarrow \delta(b) = \delta(1, b)$$
- Permutation: $gcd(d, 2^n - 1) = 1$
  $$\delta(0) = gcd(d, 2^n - 1) - 1$$

Monomials

$$\begin{array}{cccc} F_d : & \mathbb{F}_{2^n} & \to & \mathbb{F}_{2^n} \\ & x & \mapsto & x^d \end{array}$$

- $\delta(a, b)$: number of roots of $x^d + (x + a)^d = b$
- For $a \neq 0$, $\delta(a, b) = \delta(1, b/a^d)$
  $$\Rightarrow \delta(b) = \delta(1, b)$$
- Permutation: $gcd(d, 2^n - 1) = 1$
  $$\delta(0) = gcd(d, 2^n - 1) - 1$$
- Literature: Differentially 2- and 4-uniform ones

Differential Spectrum

$$\omega_i = \#\{b \in \mathbb{F}_{2^n}, \delta(b) = i\}$$

The differential spectrum of a monomial F is:

$$\mathbb{S} = \{\omega_0, \omega_2, ..., \omega_{\delta(F)}\}$$

Differential Spectrum

$$\omega_i = \#\{b \in \mathbb{F}_{2^n}, \delta(b) = i\}$$

The differential spectrum of a monomial F is:

$$\mathbb{S} = \{\omega_0, \omega_2, ..., \omega_{\delta(F)}\}$$

$$\sum_{i=0}^{\delta(F)} \omega_i = 2^n \ , \quad \sum_{i=0}^{\delta(F)} i \cdot \omega_i = 2^n$$

Differential Spectrum

$$\omega_i = \#\{b \in \mathbb{F}_{2^n}, \delta(b) = i\}$$

The differential spectrum of a monomial F is:

$$\mathbb{S} = \{\omega_0, \omega_2, ..., \omega_{\delta(F)}\}$$

$$\sum_{i=0}^{\delta(F)} \omega_i = 2^n \quad , \quad \sum_{i=0}^{\delta(F)} i \cdot \omega_i = 2^n$$

$x \mapsto x^e$ has the same differential spectrum as $x \mapsto x^d$ if:

- $e \equiv 2^k \cdot d \mod 2^n - 1$
- $e \equiv d^{-1} \mod 2^n - 1$

Outline

Differential Uniformity and Differential Spectrum

Previous work on the function $G_t(x) = x^{2^t-1}$

Spectrum of $G_t(x) = x^{2^t-1}$ when $t = \frac{n-1}{2}$ and $t = \frac{kn+1}{3}$

Conclusion

General Results on $G_t(x) = x^{2^t-1}$

[Blondeau Canteaut Charpin 2011]

- Special values:

$$\delta(0) = 2^{\gcd(t,n)} - 2, \ \delta(1) = 2^{\gcd(t-1,n)},$$

- Link with Linear Polynomials:

  $\forall b \neq 0, 1 \ \ \delta(b) = N_b - 2$ where N_b is the number of roots of:

$$P_b(x) = x^{2^t} + bx^2 + (b+1)x$$

- Link with System of Linear Equations:

$$\begin{cases} Q(y) & = & by \\ \mathbf{Tr}(y) & = & 0 \end{cases}, \ Q(y) = \sum_{i=0}^{t-1} y^{2^i}.$$

The Symmetry Property

- Restricted Spectrum:

$$\omega_i' = \#\{b \in \mathbb{F}_{2^n} \backslash \{0, 1\}, \delta(b) = i\}$$

- Symmetry:

$$G_t(x) = x^{2^{t}-1}, \qquad s = n - t + 1, \qquad G_s(x) = x^{2^{s}-1}$$

G_t and G_s have the same restricted differential spectrum

Example for $n = 14$, $G_t(x) = x^{2^t-1}$

The symmetry:

t	$\delta(0)$	$\delta(1)$	ω'_0	ω'_2	ω'_6	ω'_{14}
2	2	2	8192	8190	-	-
3	0	4	9578	6111	693	-
4	2	2	9548	6216	588	30
5	0	4	9578	6111	693	-
6	2	2	9548	6216	588	30
7	126	4	8255	8127	-	-
8	2	128	8255	8127	-	-
9	0	4	9548	6216	588	30
10	2	2	9578	6111	693	-
11	0	4	9548	6216	588	30
12	2	2	9578	6111	693	-
13	0	4	8192	8190	-	-

Example for $n = 14$, $G_t(x) = x^{2^t-1}$

Gold: $x \to x^3$ and Inverse: $x \to x^{-1}$

t	$\delta(0)$	$\delta(1)$	ω'_0	ω'_2	ω'_6	ω'_{14}
2	2	2	8192	8190	-	-
3	0	4	9578	6111	693	-
4	2	2	9548	6216	588	30
5	0	4	9578	6111	693	-
6	2	2	9548	6216	588	30
7	126	4	8255	8127	-	-
8	2	128	8255	8127	-	-
9	0	4	9548	6216	588	30
10	2	2	9578	6111	693	-
11	0	4	9548	6216	588	30
12	2	2	9578	6111	693	-
13	0	4	8192	8190	-	-

Example for $n = 14$, $G_t(x) = x^{2^t - 1}$

n even: $t = \frac{n}{2}$ $\quad$ n odd: $t = \frac{n-1}{2}$: Open

t	$\delta(0)$	$\delta(1)$	ω'_0	ω'_2	ω'_6	ω'_{14}
2	2	2	8192	8190	-	-
3	0	4	9578	6111	693	-
4	2	2	9548	6216	588	30
5	0	4	9578	6111	693	-
6	2	2	9548	6216	588	30
7	126	4	8255	8127	-	-
8	2	128	8255	8127	-	-
9	0	4	9548	6216	588	30
10	2	2	9578	6111	693	-
11	0	4	9548	6216	588	30
12	2	2	9578	6111	693	-
13	0	4	8192	8190	-	-

Example for $n = 14$, $G_t(x) = x^{2^t - 1}$

$x \to x^7$ and $x \to x^{2^{n-2}-1}$ [BCC11]

t	$\delta(0)$	$\delta(1)$	ω'_0	ω'_2	ω'_6	ω'_{14}
2	2	2	8192	8190	-	-
3	0	4	9578	6111	693	-
4	2	2	9548	6216	588	30
5	0	4	9578	6111	693	-
6	2	2	9548	6216	588	30
7	126	4	8255	8127	-	-
8	2	128	8255	8127	-	-
9	0	4	9548	6216	588	30
10	2	2	9578	6111	693	-
11	0	4	9548	6216	588	30
12	2	2	9578	6111	693	-
13	0	4	8192	8190	-	-

Example for $n = 14$, $G_t(x) = x^{2^t-1}$

$$t = \frac{n+1}{3} \text{ and } s = \frac{2n+2}{3}$$

t	$\delta(0)$	$\delta(1)$	ω'_0	ω'_2	ω'_6	ω'_{14}
2	2	2	8192	8190	-	-
3	0	4	9578	6111	693	-
4	2	2	9548	6216	588	30
5	0	4	9578	6111	693	-
6	2	2	9548	6216	588	30
7	126	4	8255	8127	-	-
8	2	128	8255	8127	-	-
9	0	4	9548	6216	588	30
10	2	2	9578	6111	693	-
11	0	4	9548	6216	588	30
12	2	2	9578	6111	693	-
13	0	4	8192	8190	-	-

Differential Spectrum of $x \mapsto x^7$ [BCC11]

- If n is odd, then:

$$\omega_6 = \frac{2^{n-2}+1}{6} - \frac{K(1)}{8}, \qquad \omega_4 = 0$$
$$\omega_2 = 2^n - 1 - 3\omega_6, \qquad \omega_0 = 2^{n-1} + 2\omega_6 + 1$$

- If n is even,

  Similar formulas but with $\omega_4 = 1$

$K(1)$ is the Kloosterman's sum:

$$K(1) = \sum_{x \in \mathbb{F}_{2^n}} (-1)^{\mathbf{Tr}(x+x^{-1})}$$

Outline

Differential Uniformity and Differential Spectrum

Previous work on the function $G_t(x) = x^{2^t-1}$

Spectrum of $G_t(x) = x^{2^t-1}$ when $t = \frac{n-1}{2}$ and $t = \frac{kn+1}{3}$

Conclusion

$G_t(x) = x^{2^t-1}$ **with** $t = \dfrac{n-1}{2}$

- Condition: n odd

$G_t(x) = x^{2^t - 1}$ with $t = \dfrac{n-1}{2}$

- Condition: n odd
- Permutation: Yes
- Differential uniformity: $\delta(G_t) = 8$ or $\delta(G_t) = 6$

$G_t(x) = x^{2^t-1}$ with $t = \dfrac{n-1}{2}$

- Condition: n odd
- Permutation: Yes
- Differential uniformity: $\delta(G_t) = 8$ or $\delta(G_t) = 6$
- Differential spectrum:

$$\text{if } n \equiv \pm 1 \bmod 6, \quad \omega_8 = 0, \quad \omega_6 = \frac{2^{n-2}+1}{6} - \frac{K(1)}{8},$$

$$\text{if } n \equiv 3 \bmod 6, \quad \omega_8 = 1, \quad \omega_6 = \frac{2^{n-2}-8}{6} - \frac{K(1)}{8},$$

$$\omega_4 = 0, \omega_2 = 2^{n-1} - 3\omega_6 - 4\omega_8 \text{ and } \omega_0 = 2^{n-1} + 2\omega_6 + 3\omega_8$$

$G_t(x) = x^{2^t-1}$ with $t = \frac{n-1}{2}$

- Condition: n odd
- Permutation: Yes
- Differential uniformity: $\delta(G_t) = 8$ or $\delta(G_t) = 6$
- Differential spectrum:

$$\text{if } n \equiv \pm 1 \bmod 6, \quad \omega_8 = 0, \quad \omega_6 = \frac{2^{n-2}+1}{6} - \frac{K(1)}{8},$$

$$\text{if } n \equiv 3 \bmod 6, \quad \omega_8 = 1, \quad \omega_6 = \frac{2^{n-2}-8}{6} - \frac{K(1)}{8},$$

$$\omega_4 = 0,\ \omega_2 = 2^{n-1} - 3\omega_6 - 4\omega_8 \text{ and } \omega_0 = 2^{n-1} + 2\omega_6 + 3\omega_8$$

- Symmetric function:

$$x \mapsto x^{2^s-1} \text{ with } s = \frac{n+3}{2}$$

Outline of the Proof (1/2)

1. Independent computation of $\delta(0)$ and $\delta(1)$.

Outline of the Proof (1/2)

1. Independent computation of $\delta(0)$ and $\delta(1)$.

2. $\forall b \neq 0, 1$, $\delta(b)$ is equal to the number of roots

$$\begin{cases} \mathcal{L}_\beta(x) & = 0 \\ \mathbf{Tr}(x^{2^t+1}) & = 1 \end{cases} \qquad \mathcal{L}_\beta(x) = x^{2^t+1} + x + \beta$$

where β is derived from b by a permutation.

Obtained in that case by studying the derivative of
$F(x) = x^\tau$ with $\tau = (2^t - 1)^{-1} \equiv -2 - 2^{t+1} \mod 2^n - 1$

[Helleseth and Kholosha 2008]

$$\mathcal{L}_\beta(x) = x^{2^t+1} + x + \beta. \qquad \mathrm{gcd}(t, n) = 1$$

[Helleseth and Kholosha 2008]

$$\mathcal{L}_\beta(x) = x^{2^t+1} + x + \beta. \qquad \gcd(t,n) = 1$$

- For any $\beta \in \mathbb{F}_{2^n}^*$, $\mathcal{L}_\beta$ has either 0, 1 or 3 roots in $\mathbb{F}_{2^n}$
- Let $M_i = \#\{\beta \in \mathbb{F}_{2^n}^*, \mathcal{L}_\beta \text{ has } i \text{ roots}\}$

  For n odd, $\quad M_0 = \frac{2^{n+1}}{3}, \quad M_1 = 2^{n-1} - 1, \quad M_3 = \frac{2^{n-1}-1}{3}.$

  For n even, $\quad M_0 = \frac{2^{n-1}}{3}, \quad M_1 = 2^{n-1}, \quad M_3 = \frac{2^{n-1}-2}{3}.$

- $\mathcal{L}_\beta$ has exactly one root $x_0 \in \mathbb{F}_{2^n}^*$ if and only if $\mathbf{Tr}\left((1 + x_0^{-1})^\tau\right) = 1$ where $\tau \equiv (2^t - 1)^{-1} \mod 2^n - 1$

Outline of the Proof (2/2)

$$\begin{cases} \mathcal{L}_\beta(x) = 0 \\ \mathbf{Tr}(x^{2^t+1}) = 1, \end{cases} \quad \mathcal{L}_\beta(x) = x^{2^t+1} + x + \beta$$

3. Computation of $\omega_0 = \#\{\beta \mid \text{system has no solution}\}$
   - $\mathcal{L}_\beta$ does not have any roots
     $\Rightarrow M_0$

Outline of the Proof (2/2)

$$\begin{cases} \mathcal{L}_\beta(x) = 0 \\ \mathbf{Tr}(x^{2^t+1}) = 1, \end{cases} \qquad \mathcal{L}_\beta(x) = x^{2^t+1} + x + \beta$$

3. Computation of $\omega_0 = \#\{\beta \mid \text{system has no solution}\}$

   - $\mathcal{L}_\beta$ does not have any roots

     $\Rightarrow M_0$

   - $\mathcal{L}_\beta$ has 1 root x_0 with $\mathbf{Tr}(x_0^{2^t+1}) \neq 1$.

     $\Rightarrow$ Formulation which involves the Kloosterman sum

Outline of the Proof (2/2)

$$\begin{cases} \mathcal{L}_\beta(x) = 0 \\ \mathbf{Tr}(x^{2^t+1}) = 1, \end{cases} \quad \mathcal{L}_\beta(x) = x^{2^t+1} + x + \beta$$

3. Computation of $\omega_0 = \#\{\beta \mid \text{system has no solution}\}$

- $\mathcal{L}_\beta$ does not have any roots
  $\Rightarrow M_0$
- $\mathcal{L}_\beta$ has 1 root x_0 with $\mathbf{Tr}(x_0^{2^t+1}) \neq 1$.
  $\Rightarrow$ Formulation which involves the Kloosterman sum
- $\mathcal{L}_\beta$ has 3 roots x_0, x_1, x_2
  It is impossible than none satisfy the trace condition
  $\Rightarrow$ Do not influence the computation of ω_0

Outline of the Proof (2/2)

$$\begin{cases} \mathcal{L}_\beta(x) = 0 \\ \mathbf{Tr}(x^{2^t+1}) = 1, \end{cases} \qquad \mathcal{L}_\beta(x) = x^{2^t+1} + x + \beta$$

3. Computation of $\omega_0 = \#\{\beta \mid \text{system has no solution}\}$
   - $\mathcal{L}_\beta$ does not have any roots

     $\Rightarrow M_0$
   - $\mathcal{L}_\beta$ has 1 root x_0 with $\mathbf{Tr}(x_0^{2^t+1}) \neq 1$.

     $\Rightarrow$ Formulation which involves the Kloosterman sum
   - $\mathcal{L}_\beta$ has 3 roots x_0, x_1, x_2

     It is impossible than none satisfy the trace condition

     $\Rightarrow$ Do not influence the computation of ω_0
4. Complete spectrum: $\sum \omega_i = 2^n$ and $\sum i \cdot \omega_i = 2^n$

$G_t(x) = x^{2^t-1}$ with $t = \dfrac{kn+1}{3}$

- Condition: $n \not\equiv 0 \mod 3$,
  $k = 1, 2$ such that t is an integer

$G_t(x) = x^{2^t-1}$ with $t = \dfrac{kn+1}{3}$

- Condition: $n \not\equiv 0 \mod 3$,
  $k = 1, 2$ such that t is an integer
- Permutation: Yes
- Differential uniformity: $\delta(G_t) = 6$

$G_t(x) = x^{2^t-1}$ with $t = \dfrac{kn+1}{3}$

- Condition: $n \not\equiv 0 \mod 3$,
  $k = 1, 2$ such that t is an integer
- Permutation: Yes
- Differential uniformity: $\delta(G_t) = 6$
- Symmetric function:

$$x \mapsto x^{2^s-1} \text{ with } s = \frac{(3-k)n+2}{3}$$

$t = \dfrac{kn+1}{3}$: Proof Elements

- $\tau = 1 + 2^t + 2^{2t}$ and

$$\begin{cases} \mathcal{L}_\beta(y) = y^{2^t+1} + y + \beta = 0, \\ \mathbf{Tr}(y^\tau) = 0 \end{cases}$$

$t = \frac{kn+1}{3}$: Proof Elements

- $\tau = 1 + 2^t + 2^{2t}$ and

$$\begin{cases} \mathcal{L}_\beta(y) = y^{2^t+1} + y + \beta = 0, \\ \mathbf{Tr}(y^\tau) = 0 \end{cases}$$

- $\omega_0 = M_0 + \#\{y \in \mathbb{F}_{2^n}, \mathbf{Tr}(y^\tau) = 1, \mathbf{Tr}\big((1 + y^{-1})^\tau\big) = 1\}$

$t = \dfrac{kn+1}{3}$: Proof Elements

- $\tau = 1 + 2^t + 2^{2t}$ and

$$\begin{cases} \mathcal{L}_\beta(y) = y^{2^t+1} + y + \beta = 0, \\ \mathbf{Tr}(y^\tau) = 0 \end{cases}$$

- $\omega_0 = M_0 + \#\{y \in \mathbb{F}_{2^n}, \mathbf{Tr}(y^\tau) = 1, \mathbf{Tr}\big((1+y^{-1})^\tau\big) = 1\}$
- Conjecture (checked for $n \leq 31$):

$$\omega_0 = M_0 + \#\{y \in \mathbb{F}_{2^n}, \mathbf{Tr}(y) = 1, \mathbf{Tr}\big(1+y^{-1}\big) = 1\}$$

$t = \frac{kn+1}{3}$: Proof Elements

- $\tau = 1 + 2^t + 2^{2t}$ and

$$\begin{cases} \mathcal{L}_\beta(y) = y^{2^t+1} + y + \beta = 0, \\ \mathbf{Tr}(y^\tau) = 0 \end{cases}$$

- $\omega_0 = M_0 + \#\{y \in \mathbb{F}_{2^n}, \mathbf{Tr}(y^\tau) = 1, \mathbf{Tr}\big((1+y^{-1})^\tau\big) = 1\}$

- Conjecture (checked for $n \leq 31$):

$$\omega_0 = M_0 + \#\{y \in \mathbb{F}_{2^n}, \mathbf{Tr}(y) = 1, \mathbf{Tr}\big(1+y^{-1}\big) = 1\}$$

- Differential spectrum (Conjecture):
  Same restricted differential spectrum than the one the functions $G_3(x) = x^7$ and $G_{\frac{n-1}{2}}(x) = x^{2^{\frac{n-1}{2}}-1}$

Outline

Differential Uniformity and Differential Spectrum

Previous work on the function $G_t(x) = x^{2^t-1}$

Spectrum of $G_t(x) = x^{2^t-1}$ when $t = \frac{n-1}{2}$ and $t = \frac{kn+1}{3}$

Conclusion

Dickson Polynomials

- Dickson Polynomials:

$$D_d(x, y): \quad D_d(x + y, xy) = x^d + y^d$$

- Reversed Dickson Polynomial: [Hou. *et al.* 2009]

$$RD_d(y) = D_d(1, y)$$

- Equivalent definition of the differential spectrum:

$$\omega_{2k} = \#\{b \in \mathbb{F}_{2^n},\ RD_d(y) = b \text{ has } k \text{ solutions in } \mathbb{F}_{2^n|\{\mathbf{Tr}(x)=0\}}\}$$

- [Göloglu 2012]: When n is even, among the functions $G_t(x) = x^{2^t - 1}$ only $G_2(x) = x^3$ is APN

Conclusion: Spectrum of $G_t(x) = x^{2^t-1}$

t	s	$\max_{b \neq 0,1} \delta(b)$	$\delta(G_t)$	$\delta(G_s)$	Spectrum
2	$n-1$	2	2	(2,4)	Gold/Inverse
$\frac{n+1}{2}$	$\frac{n+1}{2}$	2	2	2	Inverse of x^{2^t+1}

Conclusion: Spectrum of $G_t(x) = x^{2^t-1}$

t	s	$\max\limits_{b\neq 0,1} \delta(b)$	$\delta(G_t)$	$\delta(G_s)$	Spectrum
2	$n-1$	2	2	(2,4)	Gold/Inverse
$\frac{n+1}{2}$	$\frac{n+1}{2}$	2	2	2	Inverse of x^{2^t+1}
$\frac{n}{2}$	$\frac{n}{2}+1$	2	$2^{n/2-2}$	$2^{n/2}$	[BCC11]
3	$n-2$	6	6	(6,8)	[BCC11]

Conclusion: Spectrum of $G_t(x) = x^{2^t-1}$

t	s	$\max_{b\neq 0,1} \delta(b)$	$\delta(G_t)$	$\delta(G_s)$	Spectrum
2	$n-1$	2	2	(2,4)	Gold/Inverse
$\frac{n+1}{2}$	$\frac{n+1}{2}$	2	2	2	Inverse of x^{2^t+1}
$\frac{n}{2}$	$\frac{n}{2}+1$	2	$2^{n/2-2}$	$2^{n/2}$	[BCC11]
3	$n-2$	6	6	(6,8)	[BCC11]
$\frac{n-1}{2}$	$\frac{n+3}{2}$	6	(6,8)	6	This paper
$\frac{kn+1}{3}$	$\frac{(3-k)n+2}{3}$	6	6	6	This paper*

Conclusion: Spectrum of $G_t(x) = x^{2^t-1}$

t	s	$\max\limits_{b\neq 0,1} \delta(b)$	$\delta(G_t)$	$\delta(G_s)$	Spectrum
2	$n-1$	2	2	$(2,4)$	Gold/Inverse
$\frac{n+1}{2}$	$\frac{n+1}{2}$	2	2	2	Inverse of x^{2^t+1}
$\frac{n}{2}$	$\frac{n}{2}+1$	2	$2^{n/2-2}$	$2^{n/2}$	[BCC11]
3	$n-2$	6	6	$(6,8)$	[BCC11]
$\frac{n-1}{2}$	$\frac{n+3}{2}$	6	$(6,8)$	6	This paper
$\frac{kn+1}{3}$	$\frac{(3-k)n+2}{3}$	6	6	6	This paper*
$\frac{kn}{3}$	$\frac{(3-k)n+3}{3}$	6	$2^{n/3}-2$	$2^{n/3}$	– – – –